METHOD OF CIPHERING DATA TRANSMISSION IN A RADIO SYSTEM

Publication number: WO0054456 (A1)
Publication date: 2000-09-14

Inventor(s): VIALEN JUKKA [FI]; LONGONI FABIO [FI]
Applicant(s): NOKIA MOBILE PHONES LTD [FI]; VIALEN JUKKA [FI]; LONGONI FABIO [FI]

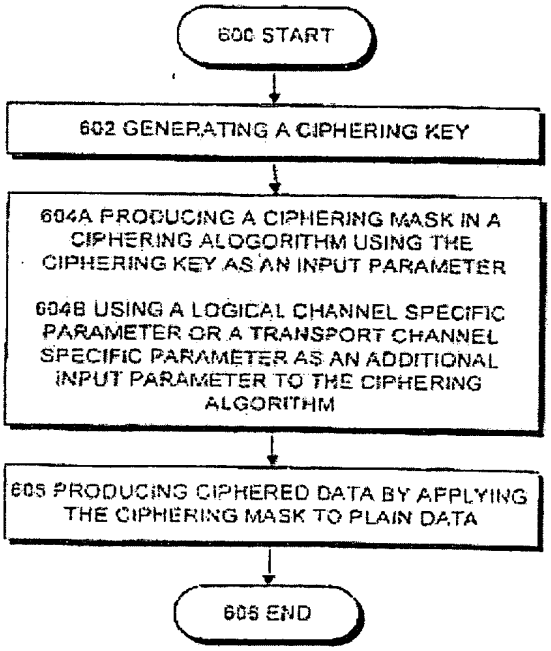
Classification:
- international: ***G09C1/00; H04L9/18; H04W12/02;*** **G09C1/00; H04L9/18; H04W12/00;** (IPC1-7): H04L9/16
- European: H04W12/02; H04L9/18
Application number: WO2000FI00177 20000308
Priority number(s): FI19990000500 19990308

Also published as:
US6882727 (B1)
US2006120530 (A1)
JP2002539490 (T)
FI990500 (A)
FI107487 (B1)
more >>

Cited documents:
WO9712461 (A1)
US5600722 (A)

Abstract of **WO 0054456 (A1)**

The invention relates to a method of ciphering data transmission in a radio system, and to a user equipment using the method, and to a radio network subsystem using the method. The method includes the steps of: (602) generating a ciphering key; (604A) producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter; (604B) using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm; and (606) producing ciphered data by applying the ciphering mask to plain data.



(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号
特表2002－539490
（P2002－539490A）
(43)公表日　平成14年11月19日(2002.11.19)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　1/00	３１０	Ｇ０９Ｃ　1/00	３１０	５Ｊ１０４
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	５Ｋ０６７

審査請求　未請求　予備審査請求　有　（全 48 頁）

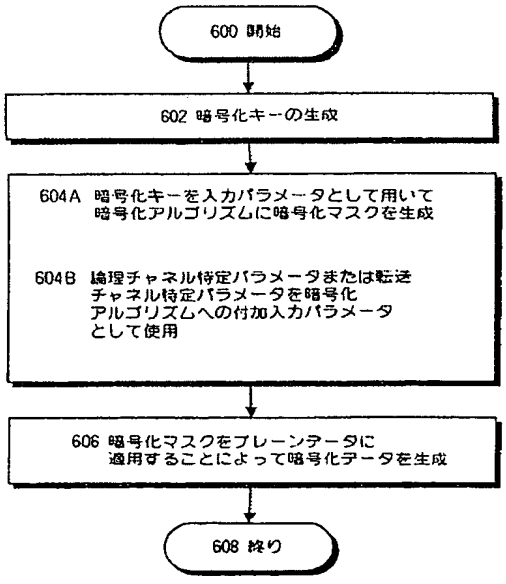
(21)出願番号　特願2000－604569(P2000－604569)
(86)（22)出願日　平成12年３月８日(2000.3.8)
(85)翻訳文提出日　平成13年９月７日(2001.9.7)
(86)国際出願番号　ＰＣＴ／ＦＩ００／００１７７
(87)国際公開番号　ＷＯ００／５４４５６
(87)国際公開日　平成12年９月14日(2000.9.14)
(31)優先権主張番号　９９０５００
(32)優先日　平成11年３月８日(1999.3.8)
(33)優先権主張国　フィンランド（ＦＩ）

(71)出願人　ノキア　モービル　フォーンズ　リミティド
フィンランド国，エフアイエヌ－02150　エスポー，ケイララーデンティエ　4
(72)発明者　ピアレン，ユッカ
フィンランド国，エフイーエン－02320　エスポー，ティルスキクヤ　3　ベー　13
(72)発明者　ロンゴニ，ファビオ
フィンランド国，エフイーエン－02130　エスポー，ピサメキ　5　エー　38
(74)代理人　弁理士　石田　敬　（外４名）

最終頁に続く

(54)【発明の名称】　無線システムのデータ伝送を暗号化する方法

(57)【要約】
本発明は、無線システムのデータ伝送を暗号化する方法と、該方法を用いるユーザ装置と、該方法を用いる無線ネットワークサブシステムとに関する。前記方法は、（６０２）暗号化キーを生成するステップと、（６０４Ａ）前記暗号化キーを入力パラメータとして用いて暗号化アルゴリズムに暗号化マスクを生成するステップと、（６０４Ｂ）前記暗号化アルゴリズムへの付加入力パラメータとして論理チャネル特定パラメータまたは転送チャネル特定パラメータを用いるステップと、（６０６）前記暗号化マスクをプレーンデータに適用することによって暗号化データを生成するステップと、を含む。



【特許請求の範囲】

【請求項１】　無線システムのデータ伝送を暗号化する方法であって、

（６０２）暗号化キーを生成するステップと、

（６０４Ａ）前記暗号化キーを入力パラメータとして用いて暗号化アルゴリズムに暗号化マスクを生成するステップと、

（６０６）前記暗号化マスクをプレーンデータに適用することによって暗号化データを生成するステップと、

を含む方法において、

（６０４Ｂ）論理チャネル特定パラメータまたは転送チャネル特定パラメータを前記暗号化アルゴリズムへの付加入力パラメータとして用いることを特徴とする、無線システムのデータ伝送を暗号化する方法。

【請求項２】　前記暗号化アルゴリズムへの付加入力パラメータとして伝送方向を用いることを特徴とする請求項１に記載の方法。

【請求項３】　前記論理チャネル特定パラメータが、無線アクセスベアラ識別子、論理チャネル識別子、信号リンク識別子の１つであることを特徴とする請求項１に記載の方法。

【請求項４】　前記転送チャネル特定パラメータが専用チャネル識別子であることを特徴とする請求項１に記載の方法。

【請求項５】　前記暗号化アルゴリズムへの付加入力パラメータとして無線フレーム特定パラメータを用いることを特徴とする請求項１に記載の方法。

【請求項６】　前記無線フレーム特定パラメータがユーザ装置フレーム番号であることを特徴とする請求項５に記載の方法。

【請求項７】　前記プレーンデータが、少なくとも２つの並列論理チャネルからの無線リンク制御レイヤプロトコルデータユニットを含み、また各論理チャネルのために個々の暗号化マスクが生成されることを特徴とする請求項１に記載の方法。

【請求項８】　少なくとも１つの論理チャネルの無線リンク制御レイヤプロトコルデータユニットがすでに暗号化され、また暗号化データを生成する前記ステップが、前記すでに暗号化された無線リンク制御レイヤプロトコルデータユニ

ットのために繰り返されないことを特徴とする請求項７に記載の方法。

【請求項９】　前記プレーンデータが、１つの論理チャネルからの１つの無線リンク制御レイヤプロトコルデータユニットを含み、また前記論理チャネルのために個々の暗号化マスクが生成されることを特徴とする請求項１に記載の方法。

【請求項１０】　前記プレーンデータが、１つの論理チャネルの少なくとも２つの連続した無線リンク制御レイヤプロトコルデータユニットを含み、また各無線リンク制御レイヤプロトコルデータユニットのために前記暗号化マスクの異なる部分が、前記暗号化データの生成に用いられることを特徴とする請求項１に記載の方法。

【請求項１１】　前記プレーンデータが、少なくとも２つの異なる論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む１つの転送ブロックセットを含み、また各転送ブロックセットのために１つの暗号化マスクが、前記暗号化データの生成に用いられることを特徴とする請求項１に記載の方法。

【請求項１２】　前記プレーンデータが、１つの論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む１つの転送ブロックセットを含み、また各転送ブロックセットのために１つの暗号化マスクが、前記暗号化データの生成に用いられることを特徴とする請求項１に記載の方法。

【請求項１３】　前記暗号化が、プロトコルスタックのメディアアクセス制御レイヤで実施されることを特徴とする請求項１に記載の方法。

【請求項１４】　新しい暗号化マスクが、前記プロトコルスタックの物理レイヤの各無線フレームのために生成されることを特徴とする請求項１に記載の方法。

【請求項１５】　新しい暗号化マスクが、前記プロトコルスタックの物理レイヤの各インタリーブ期間のために生成されることを特徴とする請求項１に記載の方法。

【請求項１６】　暗号化キー（４１０）を生成するための生成手段（４０８）と、

暗号化キー（４１０）を入力パラメータとして用いて暗号化マスク（４１２Ａ、４１２Ｂ、４１２Ｃ）を生成するための生成手段（４０８）と接続された暗号化アルゴリズム（４００）と、

暗号化マスク（４１２Ａ、４１２Ｂ、４１２Ｃ）をプレーンデータ（４１４Ａ、４１４Ｂ、４１４Ｃ）に適用することによって暗号化データ（４１８Ａ、４１８Ｂ、４１８Ｃ）を生成するための暗号化アルゴリズム（４００）と接続された暗号化手段（４１６Ａ、４１６Ｂ、４１６Ｃ）と、

を具備するユーザ装置（ＵＥ）において、

前記暗号化アルゴリズム（４００）が、論理チャネル特定パラメータ（４０２Ａ）または転送チャネル特定パラメータ（４０２Ｂ）を付加入力パラメータとして用いることを特徴とするユーザ装置。

【請求項１７】　前記暗号化アルゴリズム（４００）が、付加入力パラメータとして伝送方向を用いることを特徴とする請求項１６に記載のユーザ装置。

【請求項１８】　前記論理チャネル特定パラメータ（４０２Ａ）が、無線アクセスベアラ識別子、論理チャネル識別子、信号リンク識別子の１つであることを特徴とする請求項１６に記載のユーザ装置。

【請求項１９】　前記転送チャネル特定パラメータ（４０２Ｂ）が専用チャネル識別子であることを特徴とする請求項１６に記載のユーザ装置。

【請求項２０】　前記暗号化アルゴリズム（４００）が、無線フレーム特定パラメータ（４０４）を付加入力パラメータとして用いることを特徴とする請求項１６に記載のユーザ装置。

【請求項２１】　前記無線フレーム特定パラメータ（４０４）がユーザ装置フレーム番号であることを特徴とする請求項２０に記載のユーザ装置。

【請求項２２】　前記暗号化手段（４１６Ａ、４１６Ｂ、４１６Ｃ）が、少なくとも２つの並列論理チャネルからの無線リンク制御レイヤプロトコルデータユニットを含むプレーンデータ（４１４Ａ、４１４Ｂ、４１４Ｃ）を受け入れ、また暗号化アルゴリズム（４００）が、各論理チャネルのために個々の暗号化マスク（４１２Ａ、４１２Ｂ、４１２Ｃ）を生成し、暗号化手段（４１６Ａ、４１６Ｂ、４１６Ｃ）が、各論理チャネルのために前記チャネルの暗号化マスク（４

１２Ａ、４１２Ｂ、４１２Ｃ）を用いることを特徴とする請求項１６に記載のユーザ装置。

【請求項２３】　少なくとも１つの論理チャネルの無線リンク制御レイヤプロトコルデータユニット（４１４Ｃ）がすでに暗号化され、また暗号化手段（４１６Ｃ）が、前記すでに暗号化された無線リンク制御レイヤプロトコルデータユニット（４１４Ｃ）を暗号化しないことを特徴とする請求項２２に記載のユーザ装置。

【請求項２４】　前記暗号化手段（４１６Ａ）が、１つの論理チャネルからの無線リンク制御レイヤプロトコルデータユニットを含むプレーンデータ（４１４Ａ）を受け入れ、また暗号化アルゴリズム（４００）が、前記論理チャネルのために個々の暗号化マスク（４１２Ａ）を生成し、暗号化手段（４１６Ａ）が、前記論理チャネルのために前記チャネルの暗号化マスク（４１２Ａ）を用いることを特徴とする請求項１６に記載のユーザ装置。

【請求項２５】　前記暗号化手段（４２６）が、１つの論理チャネルの少なくとも２つの連続した無線リンク制御レイヤプロトコルデータユニットを含むプレーンデータを受け入れ、また暗号化アルゴリズム（４００）が、前記論理チャネルのために個々の暗号化マスク（４１２Ａ）を生成し、暗号化手段（４２６）が、各無線リンク制御レイヤプロトコルデータユニットのために暗号化マスク（４１２Ａ）の異なる部分を用いることを特徴とする請求項１６に記載のユーザ装置。

【請求項２６】　前記暗号化手段（４３４）が、少なくとも２つの異なる論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む１つの転送ブロックセットを含むプレーンデータを受け入れ、また暗号化アルゴリズム（４００）が、各転送ブロックセットのために個々の暗号化マスク（４１２）を生成し、暗号化手段（４３４）が、各転送ブロックセットのために１つの暗号化マスク（４１２）を用いることを特徴とする請求項１６に記載のユーザ装置。

【請求項２７】　前記暗号化手段（４３４）が、１つの論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む１つの転送ブロックセットを含むプレーンデータ受け入れ、また暗号化アルゴリズム（４００）が、各

転送ブロックセットのために個々の暗号化マスク（４１２）を生成し、暗号化手段（４３４）が、各転送ブロックセットのために１つの暗号化マスク（４１２）を用いることを特徴とする請求項１６に記載のユーザ装置。

【請求項２８】　前記生成手段（４０８）、暗号化アルゴリズム（４００）および暗号化手段（４１６Ａ、４１６Ｂ、４１６Ｃ）が、プロトコルスタックのメディアアクセス制御レイヤに存在することを特徴とする請求項１６に記載のユーザ装置。

【請求項２９】　前記暗号化アルゴリズム（４００）が、前記プロトコルスタックの物理レイヤの各無線フレームのための新しい暗号化マスク（４１２Ａ、４１２Ｂ、４１２Ｃ）を生成することを特徴とする請求項１６に記載のユーザ装置。

【請求項３０】　前記暗号化アルゴリズム（４００）が、前記プロトコルスタックの物理レイヤの各インタリーブ期間のための新しい暗号化マスク（４１２Ａ、４１２Ｂ、４１２Ｃ）を生成することを特徴とする請求項１６に記載のユーザ装置。

【請求項３１】　暗号化キー（４１０）を生成するための生成手段（４０８）と、

暗号化キー（４１０）を入力パラメータとして用いて暗号化マスク（４１２Ａ、４１２Ｂ、４１２Ｃ）を生成するための生成手段（４０８）と接続された暗号化アルゴリズム（４００）と、

暗号化マスク（４１２Ａ、４１２Ｂ、４１２Ｃ）をプレーンデータ（４１４Ａ、４１４Ｂ、４１４Ｃ）に適用することによって暗号化データ（４１８Ａ、４１８Ｂ、４１８Ｃ）を生成するための暗号化アルゴリズム（４００）と接続された暗号化手段（４１６Ａ、４１６Ｂ、４１６Ｃ）と、

を具備する無線ネットワークサブシステム（ＲＮＳ）において、

前記暗号化アルゴリズム（４００）が、論理チャネル特定パラメータ（４０２Ａ）または転送チャネル特定パラメータ（４０２Ｂ）を付加入力パラメータとして用いることを特徴とする無線ネットワークサブシステム。

【請求項３２】　前記暗号化アルゴリズム（４００）が、伝送方向を付加入

力パラメータとして用いることを特徴とする請求項３１に記載の無線ネットワークサブシステム。

【請求項３３】　前記論理チャネル特定パラメータ（４０２Ａ）が、無線アクセスベアラ識別子、論理チャネル識別子、信号リンク識別子の１つであることを特徴とする請求項３１に記載の無線ネットワークサブシステム。

【請求項３４】　前記転送チャネル特定パラメータ（４０２Ｂ）が専用チャネル識別子であることを特徴とする請求項３１に記載の無線ネットワークサブシステム。

【請求項３５】　前記暗号化アルゴリズム（４００）が、無線フレーム特定パラメータ（４０４）を付加入力パラメータとして用いることを特徴とする請求項３１に記載の無線ネットワークサブシステム。

【請求項３６】　前記無線フレーム特定パラメータ（４０４）がユーザ装置フレーム番号であることを特徴とする請求項３５に記載の無線ネットワークサブシステム。

【請求項３７】　前記暗号化手段（４１６Ａ、４１６Ｂ、４１６Ｃ）が、少なくとも２つの並列論理チャネルからの無線リンク制御レイヤプロトコルデータユニットを含むプレーンデータ（４１４Ａ、４１４Ｂ、４１４Ｃ）を受け入れ、また暗号化アルゴリズム（４００）が、各論理チャネルのために個々の暗号化マスク（４１２Ａ、４１２Ｂ、４１２Ｃ）を生成し、暗号化手段（４１６Ａ、４１６Ｂ、４１６Ｃ）が、各論理チャネルのために前記チャネルの暗号化マスク（４１２Ａ、４１２Ｂ、４１２Ｃ）を用いることを特徴とする請求項３１に記載の無線ネットワークサブシステム。

【請求項３８】　少なくとも１つの論理チャネルの無線リンク制御レイヤプロトコルデータユニット（４１４Ｃ）がすでに暗号化され、また暗号化手段（４１６Ｃ）が、前記すでに暗号化された無線リンク制御レイヤプロトコルデータユニット（４１４Ｃ）を暗号化しないことを特徴とする請求項３７に記載の無線ネットワークサブシステム。

【請求項３９】　前記暗号化手段（４１６Ａ）が、１つの論理チャネルからの無線リンク制御レイヤプロトコルデータユニットを含むプレーンデータ（４１

４Ａ）を受け入れ、また暗号化アルゴリズム（４００）が、前記論理チャネルのために個々の暗号化マスク（４１２Ａ）を生成し、暗号化手段（４１６Ａ）が、前記論理チャネルのために前記チャネルの暗号化マスク（４１２Ａ）を用いることを特徴とする請求項３１に記載の無線ネットワークサブシステム。

【請求項４０】　前記暗号化手段（４２６）が、１つの論理チャネルの少なくとも２つの連続した無線リンク制御レイヤプロトコルデータユニットを含むプレーンデータを受け入れ、また暗号化アルゴリズム（４００）が、前記論理チャネルのために個々の暗号化マスク（４１２Ａ）を生成し、暗号化手段（４２６）が、各無線リンク制御レイヤプロトコルデータユニットのために暗号化マスク（４１２Ａ）の異なる部分を用いることを特徴とする請求項３１に記載の無線ネットワークサブシステム。

【請求項４１】　前記暗号化手段（４３４）が、少なくとも２つの異なる論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む１つの転送ブロックセットを含むプレーンデータを受け入れ、また暗号化アルゴリズム（４００）が、各転送ブロックセットのために個々の暗号化マスク（４１２）を生成し、暗号化手段（４３４）が、各転送ブロックセットのために１つの暗号化マスク（４１２）を用いることを特徴とする請求項３１に記載の無線ネットワークサブシステム。

【請求項４２】　前記暗号化手段（４３４）が、１つの論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む１つの転送ブロックセットを含むプレーンデータを受け入れ、また暗号化アルゴリズム（４００）が、各転送ブロックセットのために個々の暗号化マスク（４１２）を生成し、暗号化手段（４３４）が、各転送ブロックセットのために１つの暗号化マスク（４１２）を用いることを特徴とする請求項３１に記載の無線ネットワークサブシステム。

【請求項４３】　前記生成手段（４０８）、暗号化アルゴリズム（４００）および暗号化手段（４１６Ａ、４１６Ｂ、４１６Ｃ）が、プロトコルスタックのメディアアクセス制御レイヤに存在することを特徴とする請求項３１に記載の無線ネットワークサブシステム。

【請求項４４】　前記暗号化アルゴリズム（４００）が、前記プロトコルスタックの物理レイヤの各無線フレームのための新しい暗号化マスク（４１２Ａ、４１２Ｂ、４１２Ｃ）を生成することを特徴とする請求項３１に記載の無線ネットワークサブシステム。

【請求項４５】　前記暗号化アルゴリズム（４００）が、前記プロトコルスタックの物理レイヤの各インタリーブ期間のための新しい暗号化マスク（４１２Ａ、４１２Ｂ、４１２Ｃ）を生成することを特徴とする請求項３１に記載の無線ネットワークサブシステム。

【発明の詳細な説明】

【０００１】

発明の分野

本発明は、無線システムのデータ伝送を暗号化する方法に関する。

【０００２】

発明の背景

今日、暗号化は、伝送されるデータが無資格のユーザの手に入るのを防止するために、多くのデータ伝送システムで用いられている。暗号化は、特に無線通信がより一般的になるに従い、過去数年において相当進歩している。

【０００３】

暗号化は、例えば、送信機により伝送される情報を暗号化することによって、また受信機内の情報を解読することによって、行うことができる。暗号化手段では、伝送される情報、例えばビットストリームは、ある特定数の暗号化ビットパターンによって乗算され、この場合、使用した暗号化ビットパターンが未知であるならば、元のビットストリームが何であったかを見つけだすことは困難である。

【０００４】

例えば、デジタルＧＳＭシステムでは、無線経路で暗号化が実行され、すなわち、無線経路に伝送すべき暗号化ビットストリームは、データビットと暗号化ビットとのＸＯＲをとることによって形成され、暗号化ビットは、暗号化キーＫｃを用いて、それ自体公知のアルゴリズム（Ａ５アルゴリズム）によって形成される。Ａ５アルゴリズムは、トラフィックチャネルおよびＤＣＣＨ制御チャネルで伝送される情報を暗号化する。

【０００５】

暗号化キーＫｃは、ネットワークがターミナルを認証したが、チャネル上のトラフィックがまだ暗号化されていなかった場合に設定される。ＧＳＭシステムでは、ターミナルは、ターミナルに記憶されるインターナショナルモービルサブスクライバーアイデンティティ、ＩＭＳＩ、あるいは加入者識別子に基づき形成されるテンポラリモービルサブスクライバアイデンティティ、ＴＭＳＩに基づき識

別される。加入者識別キーＫｉもターミナルに記憶される。ターミナル識別キーもシステムで認識される。

【０００６】

暗号化の信頼性が高くなるように、暗号化キーＫｃの情報は秘密に維持されなければならない。したがって、暗号化キーはネットワークからターミナルに間接的に伝送される。ランダムアクセス番号、ＲＡＮＤがネットワークに形成され、次に、その番号が基地局システムを介してターミナルに伝送される。暗号化キーＫｃは、ランダムアクセス番号、ＲＡＮＤと加入者識別キーＫｉとから公知のアルゴリズム（Ａ５アルゴリズム）によって形成される。暗号化キーＫｃは、ターミナルおよびシステムのネットワーク部分の両方において同一の方法で計算される。

【０００７】

したがって、当初は、ターミナルと基地局との間の接続におけるデータ伝送は暗号化されない。基地局システムがターミナルに暗号化モード命令を送るまで、暗号化は開始しない。ターミナルが命令を受け取ると、ターミナルは、送信すべきデータを暗号化し、受信データの解読を開始する。したがって、基地局システムは、暗号化モード命令を送信した後に受信データの解読を開始し、また暗号化された第１のメッセージをターミナルから受信しかつ正しく復号化した後に、送信されるデータの暗号化を開始する。ＧＳＭシステムでは、暗号化モード命令は暗号化の開始命令と使用するアルゴリズムに関する情報とを含む。

【０００８】

公知の方法における問題は、それらの方法が現在のシステムのために設計され、したがって、それらの方法は、１つの移動局のために複数の並列サービスが可能である新しいシステムのデータ伝送の暗号化にとって柔軟性がなく、適していないことである。同一のエアインターフェースフレームを用いて送信される２つ以上の並列プロトコルデータユニットのために同一の暗号化マスクを使用するならば、盗聴者がデータストリームから多くの情報を引き出す可能性がある。引き出すことができる情報量は、データストリームの構造に依存する。構造を持たないランダムデータから、人は情報を得ることはできないが、通常、データ内、特

に信号データ内には構造がある。

【０００９】

発明の要旨

本発明の目的は、上記の問題を解決する方法、および当該方法を実施するユーザ装置および無線ネットワークサブシステムを提供することである。上記目的は、暗号化キーを生成するステップと、暗号化キーを入力パラメータとして用いて暗号化アルゴリズムに暗号化マスクを生成するステップと、暗号化マスクをプレーンデータに適用することによって、暗号化データを生成するステップとを含む、無線システムのデータ伝送を暗号化する方法において、論理チャネル特定パラメータまたは転送チャネル特定パラメータを前記暗号化アルゴリズムへの付加入力パラメータとして用いることによって達成される。

【００１０】

本発明はまた、暗号化キーを生成するための生成手段と、暗号化キーを入力パラメータとして用いて暗号化マスクを生成するための生成手段と接続された暗号化アルゴリズムと、暗号化マスクをプレーンデータに適用することによって暗号化データを生成するための暗号化アルゴリズムと接続された暗号化手段と、を具備するユーザ装置に関する。暗号化アルゴリズムは、付加入力パラメータとして論理チャネル特定パラメータまたは転送チャネル特定パラメータを使用する。

【００１１】

さらに、本発明は、暗号化キーを生成するための生成手段と、暗号化キーを入力パラメータとして用いて暗号化マスクを生成するための生成手段と接続された暗号化アルゴリズムと、暗号化マスクをプレーンデータに適用することによって暗号化データを生成するための暗号化アルゴリズムと接続された暗号化手段と、を具備する無線ネットワークサブシステムに関する。暗号化アルゴリズムは、付加入力パラメータとして論理チャネル特定パラメータまたは転送チャネル特定パラメータを使用する。

【００１２】

本発明の好適な実施形態が、従属請求項に規定されている。

【００１３】

複数の利点が本発明によって達成される。本発明の解決策において、暗号化およびその特性を柔軟に制御できる。本発明は、新しい無線システムにおけるユーザのセキュリティを強化する。この解決方法はまた、プロトコルスタックの必要とされる機能性の分散的な実施を可能にするので、エアインターフェースフレーム毎に十分に長い暗号化マスクを一度だけ使用する公知の技術よりも優れている。

【００１４】

発明の詳細な説明

本発明は、種々の移動電話システムで用いることが可能である。以下の実施例では、本発明の利用は、本発明を汎用移動電話システム（ＵＭＴＳ）に限定することなく汎用移動電話システムについて説明する。本実施例は、ＵＭＴＳのＦＤＤ（周波数分割二重）動作を示しているが、本発明をそれに限定しない。

【００１５】

図１Ａと図１Ｂを参照して、典型的な移動電話システム構成について説明する。図１Ｂは、本発明の説明のために本質的なブロックのみを備えるが、一般の移動電話システムが他の機能および構成も備えることが当業者には明白であり、それらについて、ここでより詳細に説明する必要はない。移動電話システムの主な部分は、コアネットワークＣＮ、地球無線アクセスネットワークＵＴＲＡＮおよびユーザ装置ＵＥである。ＣＮとＵＴＲＡＮとの間のインタフェースはｌｕインタフェースと呼ばれ、ＵＴＲＡＮとＵＥとの間のインタフェースはＵｕインタフェースと呼ばれる。

【００１６】

ＵＴＲＡＮは、無線ネットワークサブシステムＲＮＳから構成される。２つのＲＮＳの間のインタフェースはｌｕｒインタフェースと呼ばれる。ＲＮＳは、無線ネットワーク制御装置ＲＮＣと１つ以上のノードＢｓＢから構成される。ＲＮＣとノードＢとの間のインタフェースはｌｕｂインタフェースと呼ばれ、ノードＢの受信領域、すなわちセルは図１ＡにＣで示されている。

【００１７】

図１Ａの表示は非常に抽象的であるので、ＵＭＴＳの部分に対応するＧＳＭシ

ステムの部分を記載することによって、図１Ｂに明瞭に示されている。ＵＭＴＳの部分の使命および機能はなお計画中なので、提示したマッピングは、決して拘束的なものではなく、推量によるものであることが明らかである。

【００１８】

図１Ｂは、移動電話システムに接続されたコンピュータ１００から、インターネット１０２を介した、ユーザ装置ＵＥに接続されたポータブルコンピュータ１２２へのパケット交換伝送を示している。ユーザ装置ＵＥは、例えば、固定装備の無線ローカルループターミナル、車両装備のターミナルまたはハンドヘルドポータブルターミナルであり得る。

【００１９】

無線ネットワークＵＴＲＡＮのインフラは、無線ネットワークサブシステムＲＮＳ、すなわち基地局サブシステムから構成される。無線ネットワークサブシステムＲＮＳは、無線ネットワーク制御装置ＲＮＣ、すなわち基地局制御装置と、少なくとも１つのノードＢ、すなわちＲＮＣ制御下の基地局とから構成される。

【００２０】

ノードＢは、マルチプレクサ１１４と、トランシーバ１１６と、トランシーバ１１６およびマルチプレクサ１１４の動作を制御する制御ユニット１１８とを備える。マルチプレクサ１１４は、複数のトランシーバ１１６によって使用されるトラフィックおよび制御チャネルを単一の伝送接続ｌｕｂに配設する。

【００２１】

ノードＢのトランシーバ１１６は、二方向（あるいは時に一方向）の無線接続Ｕｕをユーザ装置ＵＥに提供するために使用されるアンテナユニット１２０との接続部を有する。無線接続Ｕｕに伝送されるフレームの構造は詳細に決定され、また接続はエアインタフェースと呼ばれる。

【００２２】

無線ネットワーク制御装置ＲＮＣは、群中継交換フィールド１１０と制御ユニット１１２とを備える。群中継交換フィールド１１０は、スピーチとデータとを切り替えるために、また信号回路を接続するために使用される。ノードＢと無線ネットワーク制御装置ＲＮＣは基地局サブシステムを形成し、このサブシステム

は、スピーチコーデック、またはＴＲＡＵ（トランスコーダ／レートアダプタユニット）１０８としても知られるトランスコーダをさらに備える。

【００２３】

無線ネットワーク制御装置ＲＮＣとノードＢの機能と物理的構造の分割は、無線ネットワークサブシステムの実際の実現に従って異なり得る。典型的に、ノードＢは無線接続を実施する。無線ネットワーク制御装置ＲＮＣは、典型的に、無線資源管理、セル間ハンドオーバ制御、電力制御、タイミングと同期、およびユーザ装置用のページングを管理する。

【００２４】

トランスコーダ１０８は、移動交換局１０６に可能な限り近接して通常配置されるが、この理由は、それが、トランスコーダ１０８とセルラ無線ネットワーク形態の無線ネットワーク制御装置ＲＮＣとの間のスピーチ伝送を可能にし、伝送容量をセーブするからである。

【００２５】

トランスコーダ１０８は、公共交換電話網とセルラ無線ネットワークとの間で使用される異なるデジタルスピーチ符号化モードを変換して、例えば、６４ｋｂｉｔ／ｓの固定ネットワーク形態からセルラ無線ネットワークの他の形態（１３ｋｂｉｔ／ｓのような）の間で、またその逆方向で、前記公共交換電話網とセルラ無線ネットワークに互換性を与える。当然、トランスコーディングはスピーチのみのために実施される。制御ユニット１１２は、呼制御、移動度管理、統計データの収集およびシグナリングを実施する。

【００２６】

コアネットワークＣＮは、ＵＴＲＡＮの部分でない移動電話システムに属するインフラから構成される。図１Ｂは、コアネットワークＣＮ、すなわち移動交換局１０６の部分、および外界に向かう、本実施例ではインターネット１０２に向かう移動電話システムインタフェースを処理するゲートウェイ移動交換局１０４である２つの装置を示している。

【００２７】

図５は、ユーザ装置ＵＥの模範的な構造を示している。ユーザ装置ＵＥの本質

的な部分は、ユーザ装置ＵＥのアンテナ５０２、トランシーバ５０６、ユーザ装置ＵＥの制御部５１０とのインタフェース５０４、バッテリ５１４とのインタフェース５１２、およびディスプレイ５００とキーボード５０８とマイクロホン５１６とスピーカ５１８とを具備するユーザインタフェースである。

【００２８】

図２Ａは、無線送信機／無線受信機対の機能を示している。無線送信機は、ノードＢまたはユーザ装置に配置し得る。したがって、無線受信機は、ユーザ装置またはノードＢに配置し得る。

【００２９】

図２Ａの上部は、無線送信機の本質的な機能性を示している。物理チャネルに配置される異なるサービスは、例えば、スピーチ、データ、動画像または静止画像および無線送信機の制御部２１４で処理されるシステムの制御チャネルである。制御部２１４は、装置それ自体の制御および接続の制御に関係する。図２Ａは、２つの異なる転送チャネル２００Ａ、２００Ｂの操作を示している。異なるサービスは、異なるソース符号化装置を要求し、スピーチは例えばスピーチコーデックを必要とする。しかし、分かりやすくするため、ソース符号化装置は図２Ａに示さない。

【００３０】

最初に、論理チャネルはブロック２１６Ａ、２１６Ｂで暗号化される。暗号化では、暗号化されるデータは、暗号化マスクをプレーンデータに適用することによって生成される。次に、暗号化されるデータはブロック２００Ａ、２００Ｂの転送チャネルに配置される。後に図４Ａ、図４Ｃ、図７Ｂを参考にして説明するように、暗号化は、論理チャネルについてまたは転送チャネルについて実行することができる。次に、異なるチャネルは、ブロック２０２Ａと２０２Ｂでチャネル符号化される。チャネル符号化の１つの形態は異なるブロックコードであり、その１つの例は巡回冗長検査、またはＣＲＣである。チャネル符号化を実行する他の典型的な方法は、畳込み符号化およびパンクチャド畳込み符号化とターボ符号化のようなその別形態である。

【００３１】

チャネル符号化されると、チャネルはインターリーバ２０４Ａ、２０４Ｂにインターリーブされる。インターリーブの目的はエラー補正をより容易にすることである。インターリーブでは、ビットは所定の方法で互いに混合され、この結果無線経路の一時的フェーディングは、必ずしも伝達情報を識別不能にしない。

【００３２】

同一の送信機を用いて異なる信号を送信できるように、異なる信号がブロック２０８でマルチプレクスされる。

【００３３】

インターリーブされた暗号化ビットは、拡散符号で拡散され、スクランブリング符号によってスクランブルされ、またブロック２０６で変調され、その動作は図２Ｂに詳述されている。

【００３４】

最後に、組み合わせられた信号は、電力増幅器と帯域制限フィルタとを備え得る無線周波数部分２１０に搬送される。次に、アナログ無線信号がアンテナ２１２を介して無線経路Ｕｕに伝送される。

【００３５】

図２Ａの下方部分は無線受信機の典型的な機能性を示している。無線受信機は典型的にレイク（Ｒａｋｅ）受信機である。アナログ無線信号は、無線経路Ｕｕからアンテナ２３４によって受信される。受信信号は、所望の周波数帯の外側の周波数を遮断するフィルタを備える無線周波数部分２３２に搬送される。次に、信号は、復調器２２８で中間周波数または直接ベースバンドに変換され、この形態で信号は標本化かつ量子化される。

【００３６】

当該の信号はマルチパスによって伝搬された信号であるので、複数のレイクフィンガ（Ｒａｋｅ　ｆｉｎｇｅｒｓ）を備えるブロック２２８の異なるマルチパスで伝搬された信号成分を組み合わせる努力が行われる。

【００３７】

いわゆる列状のレイクフィンガでは、異なるマルチパス伝搬信号成分に関する遅延が検索される。遅延が確認された後、受信信号と、その特定のマルチパスの

確認された遅延によって遅延された使用拡散符号とを相関することによって、異なるレイクフィンガが、マルチパス伝搬信号の各々を受信するために割り当てられる。次に、復調された非拡散の異なる同一信号のマルチパスが、より強い信号を獲得するために組み合わせられる。

【００３８】

次に、受信された物理チャネルは、デマルチプレクサ２２４で異なるチャネルのデータストリームにデマルチプレクスされる。次に、チャネルの各々はデインターリーバ２２６Ａ、２２６Ｂに導かれ、ここで、受信された物理チャネルがデインターリーブされる。その後、物理チャネルは特定のチャネル復号器２２２Ａ、２２２Ｂで処理され、ここで、伝送に用いられるチャネル符号化が復号化される。畳込み符号化は、ビタビ（Ｖｉｔｅｒｂｉ）復号器によって好適に復号化される。この後、転送チャネルは、ブロック２００Ａ、２００Ｂで論理チャネルにマッピングされるか、あるいは他の可能性として、解読が転送チャネルのために実行される。チャネル復号化されたチャネル（論理または転送）は、暗号化マスクを受信データに適用することによってブロック２２０Ａ、２２０Ｂで解読される。受信された各論理チャネルは、例えば、ユーザ装置ＵＥに接続されたコンピュータ１２２にデータを転送することによって、さらに処理することができる。システムの制御チャネルは無線受信機の制御ユニット２３６に搬送される。

【００３９】

図２Ｂは、転送チャネルが符号化され、マルチプレクスされる方法を示している。原則として、図２Ｂは部分的に図２Ａと同じであるが、他の観点から示されている。ブロック２４０Ａ、２４０Ｂでは、巡回冗長検査が各転送ブロックに加えられる。インターリーブは、ブロック２４２Ａ、２４２Ｂ、２４６で２つのステージで実行される。異なる品質のサービス要求を有する２つ以上のサービスが１つ以上の物理チャネル内にマルチプレクスされる場合、サービス特定レートマッチング２４４が使用される。レートマッチングでは、チャネル記号レートは最適なレベルに調整され、ここで、各サービスのサービス要求の最低品質が同一のチャネル記号エネルギによって達成される。転送チャネルの物理チャネルへのマッピングはブロック２４８で実行される。

【００４０】

暗号化は本発明で鍵となる問題であるので、その原理について次にさらに詳細に説明する。表１では、第１の列は、受取人に伝送されなければならないプレーンデータビットを表している。第２の列のビットは暗号化マスクを構成する。暗号化マスクは、通常、排他的ＯＲ演算、すなわちＸＯＲを用いることによってプレーンデータに適用される。得られる暗号化データは第３の列にある。この暗号化データはエアインタフェースを通して受取人に送られる。次に、受取人は、送信機で用いられた同一の暗号化マスクを受信データに適用することによって、解読を実行する。第４の列は、ＸＯＲ演算を用いることによって第３の列と合計される暗号化マスクである。得られた復元データは第５の列に示される。理解されるように、復元データはプレーンデータと同じである。

【表１】

プレーンデータ	０１１１０１００１１１００１１１０００
暗号化マスク	００１０１０１０００１０００００１１１１
暗号化データ	０１０１１１１０１１０００１１１１１１
暗号化マスク	００１０１０１０００１０００００１１１１
復元データ	０１１１０１００１１１００１１１０００

【００４１】

図３は、物理チャネルで使用されるフレーム構造の実施例を示している。フレーム３４０Ａ、３４０Ｂ、３４０Ｃ、３４０Ｄには、１から７２までの連続番号が与えられ、それらは７２０ミリ秒の長さのスーパフレームを形成する。１つのフレーム３４０Ｃの長さは１０ミリ秒である。フレーム３４０Ｃは、１６のスロット３３０Ａ、３３０Ｂ、３３０Ｃ、３３０Ｄに分割される。スロット３３０Ｃの長さは０．６２５ミリ秒である。スロット３３０Ｃは、電力が例えば上方または下方に１デシベルだけ調整される１つの電力制御期間に典型的に対応する。

【００４２】

物理チャネルは、共通の物理チャネルと専用物理チャネルを含む異なる型式に分割される。

【００４３】

共通の物理チャネルは、ＰＣＨ、ＢＣＨ、ＲＡＣＨおよびＦＡＣＨの転送チャネルを搬送するために使用される。

【００４４】

専用物理チャネルは、専用物理データチャネル（ＤＰＤＣＨ）３１０と専用物理制御チャネル（ＤＰＣＣＨ）３１２とから構成される。ＤＰＤＣＨ３１０は、ＯＳＩ（開放型システム間相互接続）モデルのレイヤ２およびその上方のレイヤ、すなわち専用制御チャネル（ＤＣＨ）に生成されるデータ３０６を搬送するために使用される。ＤＰＣＣＨ３１２は、ＯＳＩモデルのレイヤ１に生成される制御情報を搬送する。制御情報は、チャネル見積もりで用いられるパイロットビット３００と、フィードバック情報（ＦＢＩ）３０８送信電力制御命令（ＴＰＣ）３０２と、選択的に転送フォーマット結合インジケータ（ＴＦＣＩ）３０４とを含む。ＴＦＣＩ３０４は、現在のフレームで用いられている異なる転送チャネルの転送フォーマット、すなわち転送フォーマット結合について受信機に知らせる。

【００４５】

図３から分かるように、ダウンリンクＤＰＤＣＨ３１０とＤＰＣＣＨ３１２は、同一のスロット３３０Ｃにタイムマルチプレクスされる。アップリンクでは、チャネルが各フレーム３４０Ｃにマルチプレクスされる１Ｑ／コード（Ｉ＝同相、Ｑ＝直角位相）であるように、チャネルは並列に送られる。

【００４６】

無線インタフェースＵｕのチャネルは、ＩＳＯ（国際標準化機構）のＯＳＩ（開放型システム間相互接続）モデルに従って、３つのプロトコルレイヤ、物理レイヤ（＝レイヤ１）、データリンクレイヤ（＝レイヤ２）およびネットワークレイヤ（＝レイヤ３）を含むプロトコルアーキテクチャに従って処理される。プロトコルスタックは、無線ネットワークサブシステムＲＮＳおよびユーザ装置ＵＥの両方に配置されている。各ユニット（例えば、ユーザ装置または無線ネットワ

ークサブシステム）は、他のユニットのレイヤと論理的に通信するレイヤを有する。最も低い物理レイヤのみが互いに直接連通する。他のレイヤは、常に、次の下方のレイヤについて提供されるサービスを使用する。かくして、メッセージは、レイヤの間に垂直方向に物理的に通過しなければならず、また最も低いレイヤのみでメッセージはレイヤの間を水平に通過する。図７Ａはプロトコルアーキテクチャのレイヤを示している。異なるサブレイヤの間の楕円形は、サービスアクセスポイント（ＳＡＰ）を示している。

【００４７】

物理レイヤＬ１は、ＭＡＣのサブレイヤＭＡＣおよび高次のレイヤに異なる転送チャネルを提供する。如何にまたどのような特性によって、データが無線インタフェースで転送されるかについて、物理レイヤ転送サービスを説明する。転送チャネルは、ページングチャネルＰＣＨ、放送チャネルＢＣＨ、同期チャネルＳＣＨ、ランダムアクセスチャネルＲＡＣＨ、順方向アクセスチャネルＦＡＣＨ、ダウンリンク共用チャネルＤＳＣＨ、高速アップリンク信号チャネルＦＡＵＳＣＨおよび専用チャネルＤＣＨを含む。物理レイヤＬ１は、物理チャネルによって転送チャネルをマッピングする。ＦＤＤ（周波数分割二重）モードでは、物理チャネルはコード、周波数によって、アップリンクでは、相対位相（Ｉ／Ｑ）によって特徴づけられる。ＴＤＤ（時分割二重）モードでは、物理チャネルはまた、タイムスロットによって特徴づけられる。

【００４８】

転送チャネルは、共通チャネル（特定のＵＥがアドレスされたときにＵＥのインバンド識別の必要がある場合）と、専用チャネル（ＵＥが、物理チャネル、すなわちＦＤＤとコードに関するコードと周波数、ＴＤＤに関するタイムスロットおよび周波数によって識別される場合）とに分割し得る。

【００４９】

共通の転送チャネルの型式は次の通りである。ＲＡＣＨは、例えば、初期アクセスまたは非リアルタイム専用制御またはトラフィックデータのかなり少量のデータを伝送するために使用される競合ベースのアップリンクチャネルである。ＦＡＣＨは、かなり少量のデータを伝送するために使用される、閉ループ電力制御

なしの共通のダウンリンクチャネルである。ＤＳＣＨは、専用制御またはトラフィックデータを搬送する複数のＵＥと共有されるダウンリンクチャネルである。ＢＣＨは、システム情報をセル全体に放送するために使用されるダウンリンクチャネルである。ＳＣＨは、ＴＤＤモードで同期情報をセル全体に放送するために使用されるダウンリンクチャネルである。ＰＣＨは、制御情報をセル全体に放送するために使用されるダウンリンクチャネルであり、効率的なＵＥスリープモード手順を可能にする。

【００５０】

次に、専用転送チャネルの型式は次の通りである。ＤＣＨは、アップリンクまたはダウンリンクで用いられる１つのＵＥ専用のチャネルである。ＦＡＵＳＣＨは、ＦＡＣＨに関連して専用チャネルを割り当てるために使用されるアップリンクチャネルである。データリンクレイヤは、２つのサブレイヤ、すなわちＭＡＣサブレイヤ（メディアアクセス制御）およびＲＬＣサブレイヤ（無線リンク制御）に分割される。ＭＡＣサブレイヤＬ２／ＭＡＣは、ＲＬＣサブレイヤＬ２／ＲＬＣに異なる論理チャネルを提供する。論理チャネルは、転送される情報の種類によって特徴づけられる。論理チャネルは、ページング制御チャネルＰＣＣＨ、放送制御チャネルＢＣＣＨ、同期制御チャネルＳＣＣＨ、共通制御チャネル、専用制御チャネルＤＣＣＨおよび専用トラフィックチャネルＤＴＣＨを含む。

【００５１】

制御チャネルは、制御プレーン情報のみの転送のために使用される。ＳＣＣＨは、ＴＤＤ（時分割二重）動作の場合に同期情報を放送するためのダウンリンクチャネルである。ＢＣＣＨは、システム制御情報を放送するためのダウンリンクチャネルである。ＰＣＣＨは、ページング情報を転送するダウンリンクチャネルである。ＣＣＣＨは、ネットワークとＵＥとの間に制御情報を伝送するための双方向チャネルである。このチャネルは、ネットワークとのＲＲＣ接続を持たないＵＥによって共通に使用される。ＤＣＣＨは、ＵＥとネットワークとの間に専用制御情報を伝送する点から点の双方向チャネルである。このチャネルは、ＲＲＣ接続セットアップ手順を通して確立される。

【００５２】

トラフィックチャネルは、ユーザプレーンの情報のみの転送のために使用される。ＤＴＣＨは、ユーザ情報の転送のための、１つのＵＥ専用の点から点のチャネルである。ＤＴＣＨは、アップリンクとダウンリンクの両方に存在できる。

【００５３】

ＭＡＣレイヤは、転送チャネルによって論理チャネルをマッピングする。ＭＡＣサブレイヤの機能の１つは、瞬時ソースビットレートに依存する各転送チャネルのために適切な転送フォーマットを選択することである。

【００５４】

図７Ｃは、論理チャネルと転送チャネルとの間のマッピングを示している。ＳＣＣＨはＳＣＨに接続されている。ＢＣＣＨはＢＣＨに接続されている。ＰＣＣＨがＰＣＨに接続された。ＣＣＣＨはＲＡＣＨとＦＡＣＨとに接続されている。ＤＴＣＨは、ＲＡＣＨとＦＡＣＨとに、ＲＡＣＨとＤＳＣＨとに、ＤＣＨとＤＳＣＨとに、あるいはＤＣＨに接続できる。ＤＣＣＨは、ＲＡＣＨとＦＡＣＨとに、ＲＡＣＨとＤＳＣＨとに、ＤＣＨとＤＳＣＨとに、ＤＣＨに、あるいはＦＡＵＳＣＨに接続できる。

【００５５】

第３のレイヤＬ３は、ユーザ装置とネットワークとの間のレイヤ３の制御プレーン信号を処理するＲＲＣサブレイヤ（無線資源制御）を有する。ＲＲＣサブレイヤによって実施される機能には、ＲＲＣ接続のための無線資源の割り当て、再構成および解放がある。したがって、ＲＲＣサブレイヤは、制御およびユーザプレーンの両方の要求を含むＲＲＣ接続に必要な無線資源の割り当てを処理する。ＲＲＣレイヤは、ＲＲＣ接続の確立中に無線資源を再構築し得る。

【００５６】

本発明において、我々は、一人のユーザの異なるサービスのデータフローの暗号化に関心がある。公知の技術によれば、すべてのデータフローは、同一の暗号化マスクを使用して暗号化される。

【００５７】

無線システムのデータ伝送を暗号化するための本発明による方法が、図６に示されている。本方法の実行は、ブロック６００において始まる。

【００５８】

ブロック６０２では、暗号化キーは、例えば本発明の背景部分に記述されているような公知の技術に従って生成される。

【００５９】

ブロック６０４Ａでは、暗号化マスクは、暗号化キーを入力パラメータとして用いて暗号化アルゴリズムに生成される。論理チャネル特定パラメータまたは転送チャネル特定パラメータはまた、暗号化アルゴリズムへの付加入力パラメータとして用いられる。論理チャネル特定パラメータは、無線アクセスベアラ識別子、論理チャネル識別子、信号リンク識別子、または使用チャネルを識別する他のあるパラメータの１つであり得る。転送チャネルの特定のパラメータは使用された転送チャネルを識別する、例えば、専用チャネル呼識別子、あるいは何か他のパラメータであり得る。

【００６０】

用語「ベアラ」は、ネットワークサービスに関連して使用される情報を伝送するための高レベルの名称である。サービスに応じて、１つ以上のベアラを用いてＵＭＴＳの情報を通常伝送することができる。例えば、サービスは、スピーチ伝送、データサービスおよびビデオサービスを含む。他方、無線ベアラは、エアインタフェースにわたって展開するベアラのその部分を表す。１つの論理チャネルは通常１つの無線ベアラを搬送する。論理チャネルは、ＭＡＣレイヤによって提供されるサービスを規定する。論理チャネルは、既存のサービスモードに応じて、異なる種類の転送チャネルにマッピングすることができる（専用転送チャネルまたは共通転送チャネルに）。転送チャネルは、物理レイヤによって提供されるサービスを規定する。複数の論理チャネルをＭＡＣレイヤの１つの転送チャネルにマルチプレクスすることも可能である。さらに、転送チャネルは、物理レイヤの物理チャネルにマッピングされる。複数の転送チャネルは、レイヤ１によって１つの物理チャネルにマルチプレクスすることができる。転送チャネルのマルチプレクスの後に、データストリームを複数の物理チャネルの間に分割することが可能である。

【００６１】

かくして、１つ以上の並列の無線ベアラを用いて他のトランシーバとターミナルが無線できる無線システムに、本発明を適用することができる。典型的に、呼出しがターミナルとネットワークとの間に確立されるとき、ターミナルと無線ネットワークサブシステムとの間のシグナリング無線ベアラＳＲＢのために物理チャネルが最初に確立され、このチャネルが一旦確立されると、１つまたは複数の実際のトラフィックベアラを確立することができる。ＳＲＢは、信号リンクとも呼ぶことができる。

【００６２】

伝送の方向（アップリンク／ダウンリンク）は、暗号化アルゴリズムへの付加入力パラメータとして使用することができる。

【００６３】

さらにもう１つのパラメータが存在し、すなわち、暗号化アルゴリズムへの付加入力パラメータとして無線フレーム特定パラメータを使用することができる。無線フレーム特定パラメータは、例えば、ユーザ装置フレーム番号（ＵＥＦＮ）、または使用無線フレームを識別する他のあるパラメータであり得る。無線フレーム特定パラメータは、暗号化機能が実施されるプロトコルレイヤに依存する。暗号化機能が、ＵＥとＣＮに終端するプロトコルレイヤで実施されるならば、使用フレーム番号を受信体に搬送するための機構を規定しなければならない。暗号化機能がＭＡＣレイヤまたはレイヤ１（あるいはＵＥとノードＢまたはＲＮＣに終端する他のあるレイヤ）に配置されるならば、少なくとも部分的に物理フレーム番号から成るフレーム番号を使用することができ、これは、使用フレーム番号をデータで信号伝送する必要がないことを意味する。

【００６４】

ブロック６０６では、暗号化データは、例えば表１に示したようなＸＯＲ演算を用いて、暗号化マスクをプレーンデータに適用することによって生成される。

【００６５】

次に、送信機および受信機における暗号化方法の実施を示した詳細な実施例について、図４Ａ、図４Ｂ、図４Ｃに関連して説明する。関連する点についてのみ示すが、例えば異なった数のＰＤＵを有する多様な状態で暗号化を実行できるこ

とが当業者には明らかであろう。

【００６６】

図４Ａは、本発明で規定された基本的な暗号化環境を規定するブロック図を示している。生成手段４０８は、公知の技術による暗号化キー４１０を生成するために使用される。生成手段４０８には、暗号化マスク４１２Ａ、４１２Ｂ、４１２Ｃを生成するための暗号化アルゴリズム４００が接続されている。暗号化アルゴリズムは、生成された暗号化キー４１０を入力パラメータとして使用する。暗号化アルゴリズム４００は、付加入力パラメータとして論理チャネル特定パラメータ４０２Ａを使用する。

【００６７】

受信機端末では、解読のために必要な論理チャネル特定パラメータを、暗号化されていないＭＡＣヘッダから、例えばＭＡＣヘッダのＣ／Ｔフィールドから読み取ることができる。ＭＡＣ　ＰＤＵの構造が図８に示されている。ＭＡＣ　ＰＤＵは、任意のＭＡＣヘッダ８００とＭＡＣサービスデータユニット（ＭＡＣ　ＳＤＵ）８０２とから構成される。ＭＡＣヘッダおよびＭＡＣ　ＳＤＵの両方のサイズは可変である。ＭＡＣヘッダ８００の内容とサイズは、論理チャネルの型式に依存し、ある場合にはどのパラメータもＭＡＣヘッダ８００に必要でない。ＭＡＣ－ＳＤＵ８０２のサイズは、セットアップ手順の間に規定されるＲＬＣ　ＰＤＵのサイズに依存する。ＭＡＣヘッダ８００はＣ／Ｔフィールド８０４を備える。この選択は、異なる論理チャネル（または同一の論理チャネル型式の異なるインスタンス）を１つの転送チャネルに、専用転送チャネルと共通転送チャネルの両方に、効率的にＭＡＣマルチプレクスするのを可能にする。この方法を使用する場合、ＭＡＣヘッダは暗号化されず、これによって、受信機端末の異なるＭＡＣ　ＰＤＵの分離が可能になり、また共通チャネルモードでは、ＵＴＲＡＮの正しい実体にメッセージをルーチンするために必要なＲＮＴＩ（無線ネットワーク一時識別子）フィールドの読取りが可能になる。

【００６８】

暗号化アルゴリズム４００には、暗号化マスク４１２Ａ、４１２Ｂ、４１２Ｃをプレーンデータ４１４Ａ、４１４Ｂ、４１４Ｃに適用することによって、暗号

化データ４１８Ａ、４１８Ｂ、４１８Ｃを生成するための暗号化手段４１６Ａ、４１６Ｂ、４１６Ｃが接続されている。図４Ａから分かるように、プレーンデータは、少なくとも２つの並列論理チャネルからの無線リンク制御レイヤプロトコルデータユニットを含み、また各論理チャネルのために個々の暗号化マスクが生成される。したがって、図４Ａでは、したがって、暗号化マスク４１２Ａ、４１２Ｂおよび４１２Ｃはすべて互いに異なる。

【００６９】

ブロック４２０では、暗号化されたＲＬＣ－ＰＤＵは、ＭＡＣレイヤを通して処理され、１つの転送ブロックセット、すなわちＭＡＣ　ＰＤＵセットにマッピングされる。

【００７０】

他の可能な解決策は、プレーンデータが、１つのみの論理チャネルからの１つの無線リンク制御レイヤプロトコルデータユニット４１４Ａを含む解決策であり、また前記論理チャネルのために個々の暗号化マスク４１２Ａが生成される。したがって、本発明はまた個々の論理チャネルのためにも機能する。

【００７１】

通常、プロトコルスタックの物理レイヤの各無線フレームのために、新しい暗号化マスクが生成される。インターリーブが使用されるならば、プロトコルスタックの物理レイヤの各インターリーブ期間について新しい暗号化マスクを生成することができる。典型的に、１つのインターリーブ期間は複数の無線フレームから構成される。

【００７２】

図４Ａの左側は、送信機で実施される動作を示している。図４Ａの右側に示されているように、対応する動作は受信機においても実施される。唯一の差は、受信された転送ブロックセットからＲＬＣ－ＰＤＵを導くためにブロック４２２が使用されることであり、また受信データを解読するために解読手段４２４Ａ、４２４Ｂ、４２４Ｃが使用されることである。

【００７３】

本発明の１つの実施形態では、少なくとも１つ論理チャネルの無線リンク制御

レイヤプロトコルデータユニットは、すでに暗号化されており、また暗号化データを生成するステップは、前記すでに暗号化された無線リンク制御レイヤプロトコルデータユニットのために繰り返されない。かくして、データを２度暗号化することが避けられる。当然、例えばこのような端末から端末への暗号化が使用されるならば、データを２度、すなわち最初にサービスを用いた適用によって、次に本発明によるＭＡＣレイヤによって暗号化することができる。これによって、たとえ暗号化が２度実行されるとしても、ＸＯＲ演算は余分のビットを加えないので、送信容量の損失は引き起こされない。

【００７４】

図４Ｂは、プレーンデータが、１つの論理チャネルの少なくとも２つの連続した無線リンク制御レイヤプロトコルデータユニットを含む状態に対する解決策を示している。例えば、第１のＲＬＣ　ＰＤＵ４１４Ａおよび第２のＲＬＣ　ＰＤＵ４１４Ｂが１つの論理チャネルからであると仮定するならば、問題は、これらのＰＤＵ４１４Ａ、４１４Ｂのために１つのみの暗号化マスク４１２Ａを生成するような方法で解決することができる。次に、この暗号化マスク４１２Ａの異なる部分は、第１のＰＤＵ４１４Ａと第２のＰＤＵ４１４Ｂとを暗号化するために使用される。この場合に必要な暗号化マスク４１２Ａの長さは、当然、第１および第２のＰＤＵ４１４Ａ、４１４Ｂの長さの和である。ＰＤＵ４１４Ａ、４１４Ｂは同一の論理チャネル（同一の無線アクセスベアラ）からなので、必要とされる最大長は、そのベアラの最大ＲＬＣ　ＰＤＵサイズの２倍であると計算され得る。

【００７５】

図４Ｃは、プレーンデータが、少なくとも２つの異なる論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む１つの転送ブロックセット（ＴＢＳ）を有する状態を示し、各転送ブロックセットのために、暗号化データを生成する際に１つの暗号化マスク４１２が使用される。この選択では、暗号化される基本単位は転送ブロックセットである。これは、アルゴリズム４００によって製造される暗号化マスク４１２の必要な長さを規定する。レイヤ１は、転送ブロック特定のＣＲＣ（巡回冗長検査）をなお加えるが、ＸＯＲ演算はデータ

の長さを変えないので、ＴＢＳ全体を１つの単位として暗号化できなければならない。ＴＢＳの各転送ブロックの長さは、いずれにせよＬ１に伝えなければならない。この選択は、ＭＡＣヘッダもまた暗号化され、したがって、ＴＢＳを解読する前に、ＭＡＣ　ＰＤＵをネットワーク側のどこにも導くことができないという不都合を有する。これは、ｌｕｒ上の共通チャネルが可能であるならば、問題である。必要な暗号化マスク４１２の長さは、当該の転送チャネルのための最大転送ブロックセットサイズに等しい。

【００７６】

他の可能な解決策は、プレーンデータが、１つの論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む解決策であり、各転送ブロックセットのために、暗号化データを生成する際に１つの暗号化マスク４１２が使用される。

【００７７】

本発明の解決策は、好ましくはソフトウェアによって無線システムで実施され、この場合、本発明は、送信機および受信機に、特に図２Ａのブロック２０４Ａ、２０４Ｂおよび２２６Ａ、２２６Ｂに配置されるプロトコル処理ソフトウェアに、ある機能を必要とする。かくして、生成手段４０８、暗号化アルゴリズム４００および暗号化手段４１６Ａ、４１６Ｂ、４１６Ｃは、ユーザ装置ＵＥおよび無線ネットワークサブシステムＲＮＳに存在するプロトコルスタックのソフトウェアモジュールであり得る。解決策はまた、例えばＡＳＩＣ（特定用途向け集積回路）または別個のコンポーネントを用いてハードウェアによって実施することができる。

【００７８】

本発明の方法は、例えば、プロトコルスタックのメディアアクセス制御レイヤで実施することができる。これは図７Ｂに示され、本図は、含まれる暗号化機能について図７Ａに示されたＭＡＣレイヤの高レベルの概要を示している。Ｃ１（）およびＣ２（）は、暗号化の位置の２つの選択肢である。Ｃ１（０）、Ｃ１（１）、Ｃ１（２）およびＣ１（３）は、図４Ａと図４Ｂを参考にして上に説明したような論理チャネル特定暗号化パラメータの使用を示し、これに対し、Ｃ２（

００）、Ｃ２（０１）およびＣ２（０２）は転送チャネル特定暗号化パラメータの使用を示している。あるＭＡＣ機能がＣ２（００）、Ｃ２（０１）およびＣ２（０２）ブロックの下で必要とされるかもしれないが、分かりやすさのため、それらはここでは図示しない。基本的に、ＲＬＣ　ＰＤＵは各論理チャネルからＭＡＣレイヤに来る。ＭＡＣレイヤでは、次に、ＲＬＣ－ＰＤＵは、ＰＣＨ、ＢＣＨ、ＳＣＨ、専用チャネル用の動作および共通チャネル動作を含む機能ブロック７００、７０２、７０４においてＭＡＣ　ＰＤＵにマッピングされる。通常、１つのＲＬＣ　ＰＤＵは１つのＭＡＣ　ＰＤＵ（＝転送ブロック）にマッピングされる。このマッピングによって、論理チャネルから転送チャネルへのマッピングが実現される。マッピング規則は図７Ｃに関連して上に説明してある。暗号化がＣＣＣＨのために使用されるならば、暗号化ブロック、例えばＣ１（４）は、図７Ｂで「ＣＣＣＨ」と機能ブロック７０４との間のラインの中になければならない。

【００７９】

本発明について、添付図面に示した実施例を参考にして上に記述してきたが、本発明がその実施例に限定されず、添付請求項に開示した創意に富んだ構想内の多くの方法で変更し得ることが明白である。

【図面の簡単な説明】

【図１Ａ】

移動電話システムの例（その１）である。

【図１Ｂ】

移動電話システムの例（その２）である。

【図２Ａ】

送信機と受信機を示している。

【図２Ｂ】

転送チャネルの符号化および多重化を示している。

【図３】

フレーム構造を示している。

【図４Ａ】

本発明による暗号化環境のブロック図（その１）である。

【図４Ｂ】

本発明による暗号化環境のブロック図（その２）である。

【図４Ｃ】

本発明による暗号化環境のブロック図（その３）である。

【図５】

移動局を示している。

【図６】

本発明による方法を示したフローチャートである。

【図７Ａ】

プロトコルスタックの例を示している。

【図７Ｂ】

本発明によるプロトコルスタックの例を示している。

【図７Ｃ】

論理チャネルと転送チャネルとの間のマッピングを示している。

【図８】

メディアアクセス制御レイヤプロトコルデータユニットの構造を示している。

【図１Ａ】

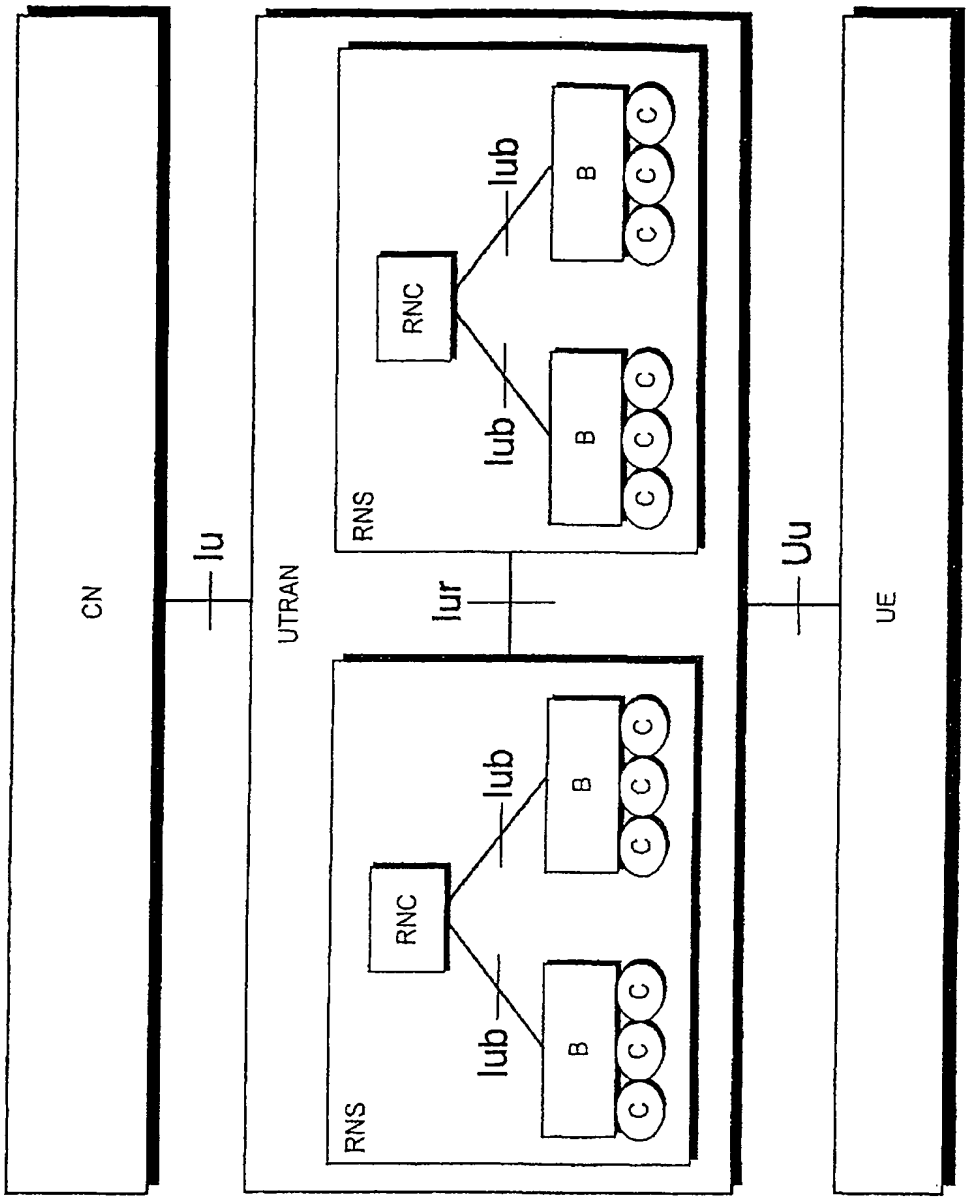


Fig 1A

【図１Ｂ】

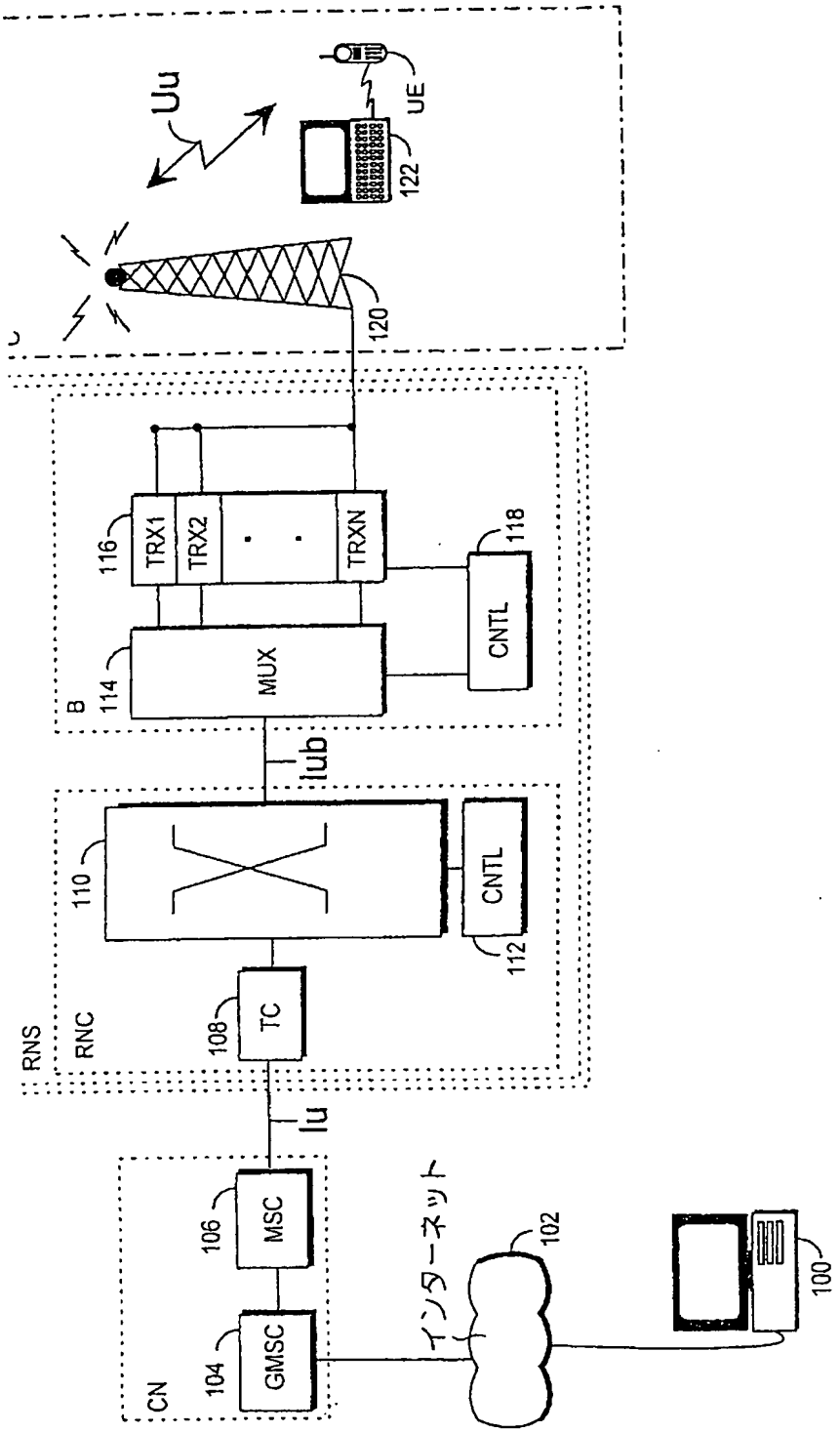

Uu
UE
122
120
C
116
TRX1
TRX2
TRXN
118
CNTL
114
MUX
B
Iub
110
CNTL
112
108
TC
RNC
RNS
Iu
106
MSC
104
GMSC
CN
インターネット
102
100

Fig 1B

【図２Ａ】

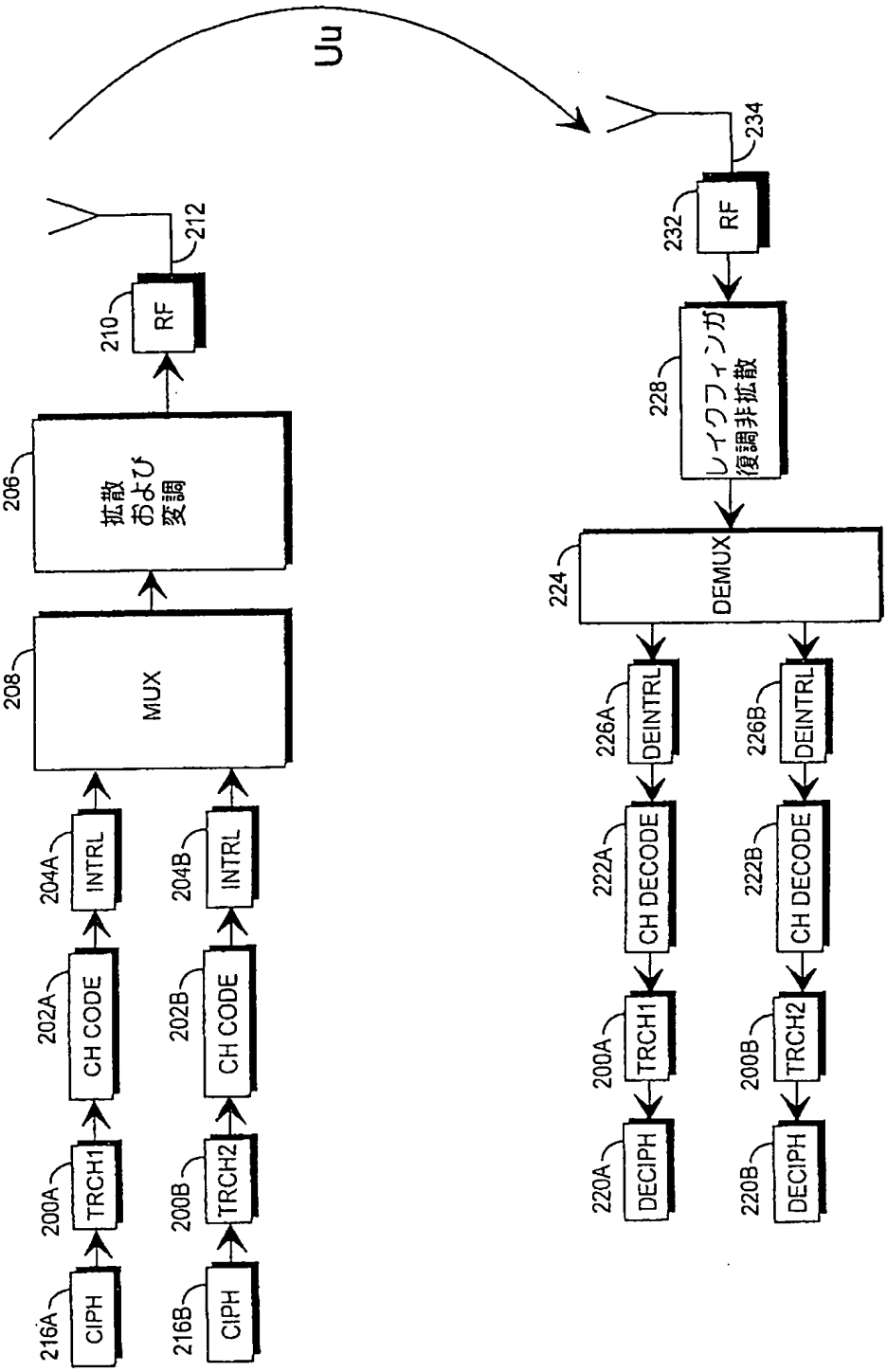

Uu
212
RF
210
拡散
および
変調
206
MUX
208
INTRL
204A
CH CODE
202A
TRCH1
200A
CIPH
216A
INTRL
204B
CH CODE
202B
TRCH2
200B
CIPH
216B
234
RF
232
レイクフィンガ
復調非拡散
228
DEMUX
224
DEINTRL
226A
CH DECODE
222A
TRCH1
200A
DECIPH
220A
DEINTRL
226B
CH DECODE
222B
TRCH2
200B
DECIPH
220B

Fig 2A

【図２Ｂ】

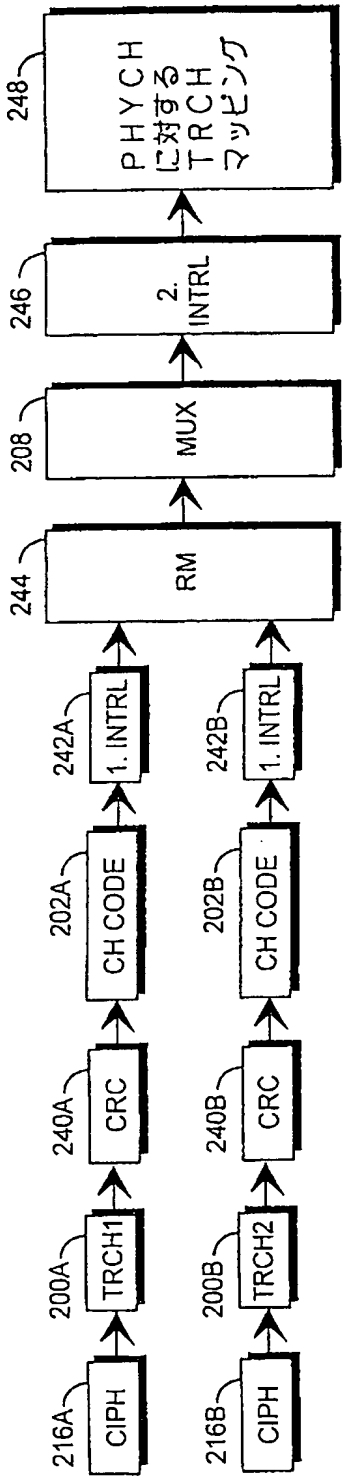

248
PHYCHに対するTRCHマッピング
246
2. INTRL
208
MUX
244
RM
242A
1. INTRL
242B
1. INTRL
202A
CH CODE
202B
CH CODE
240A
CRC
240B
CRC
200A
TRCH1
200B
TRCH2
216A
CIPH
216B
CIPH

Fig 2B

【図３】

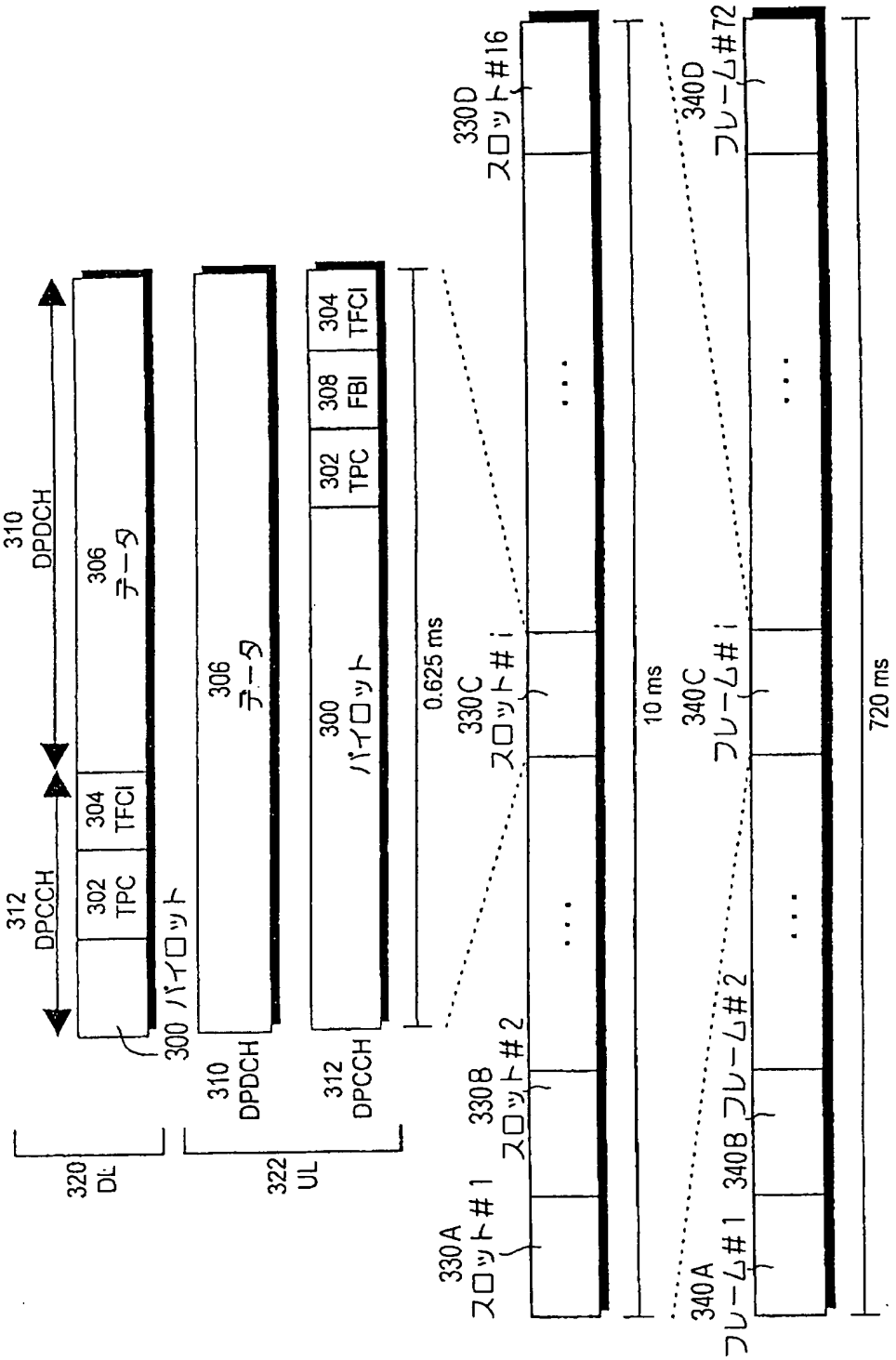

320
DL
322
UL
312
DPCCH
302
TPC
304
TFCI
310
DPDCH
306
データ
300
パイロット
308
FBI
0.625 ms
330A
スロット#1
330B
スロット#2
330C
スロット#i
330D
スロット#16
10 ms
340A
フレーム#1
340B
フレーム#2
340C
フレーム#i
340D
フレーム#72
720 ms

Fig 3

【図４Ａ】

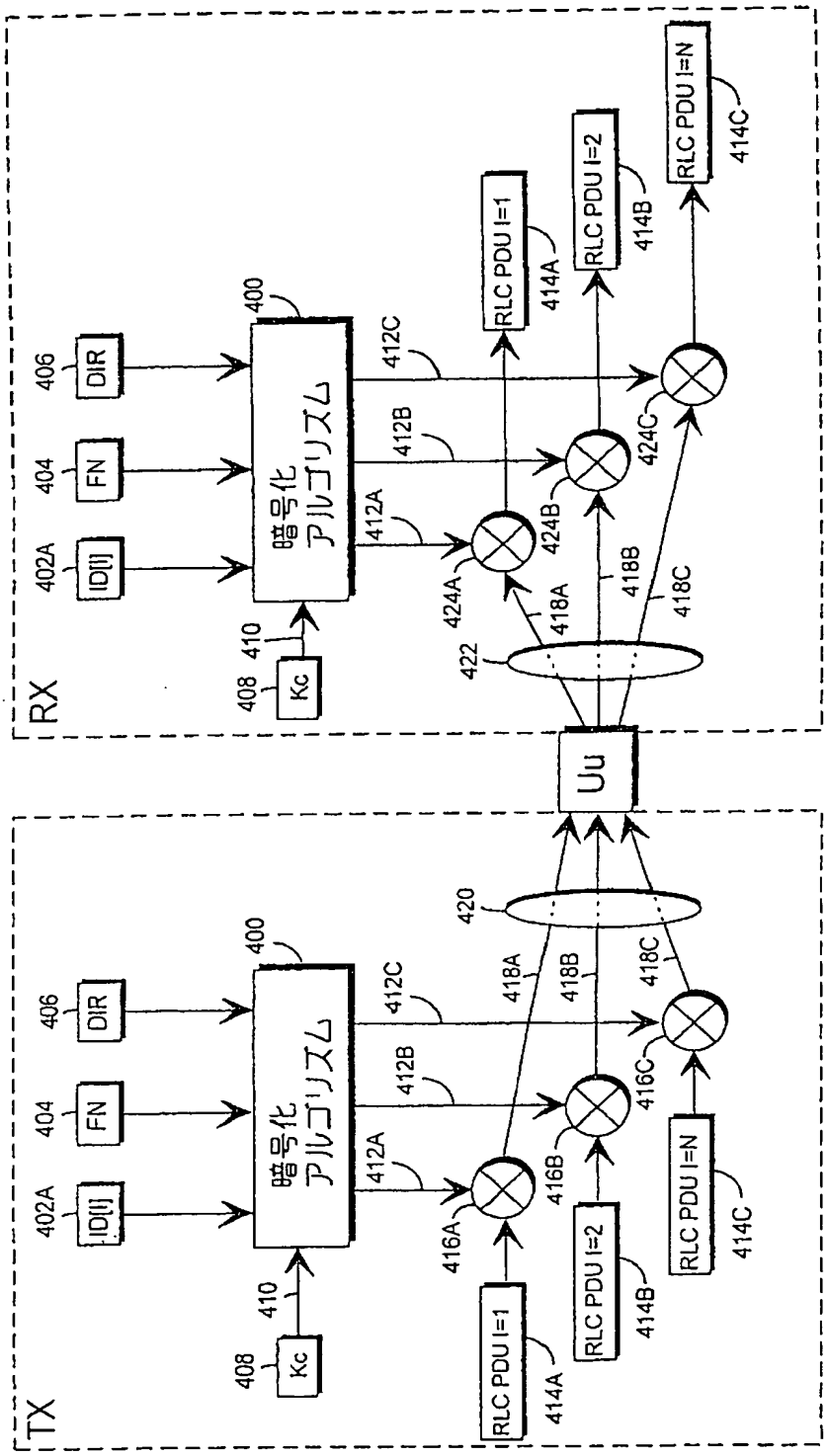

RX
TX
Uu
暗号化アルゴリズム
400
406
DIR
404
FN
402A
ID[i]
408
Kc
410
412A
412B
412C
418A
418B
418C
420
422
424A
424B
424C
416A
416B
416C
414A
414B
414C
RLC PDU I=1
RLC PDU I=2
RLC PDU I=N

Fig 4A

【図４Ｂ】

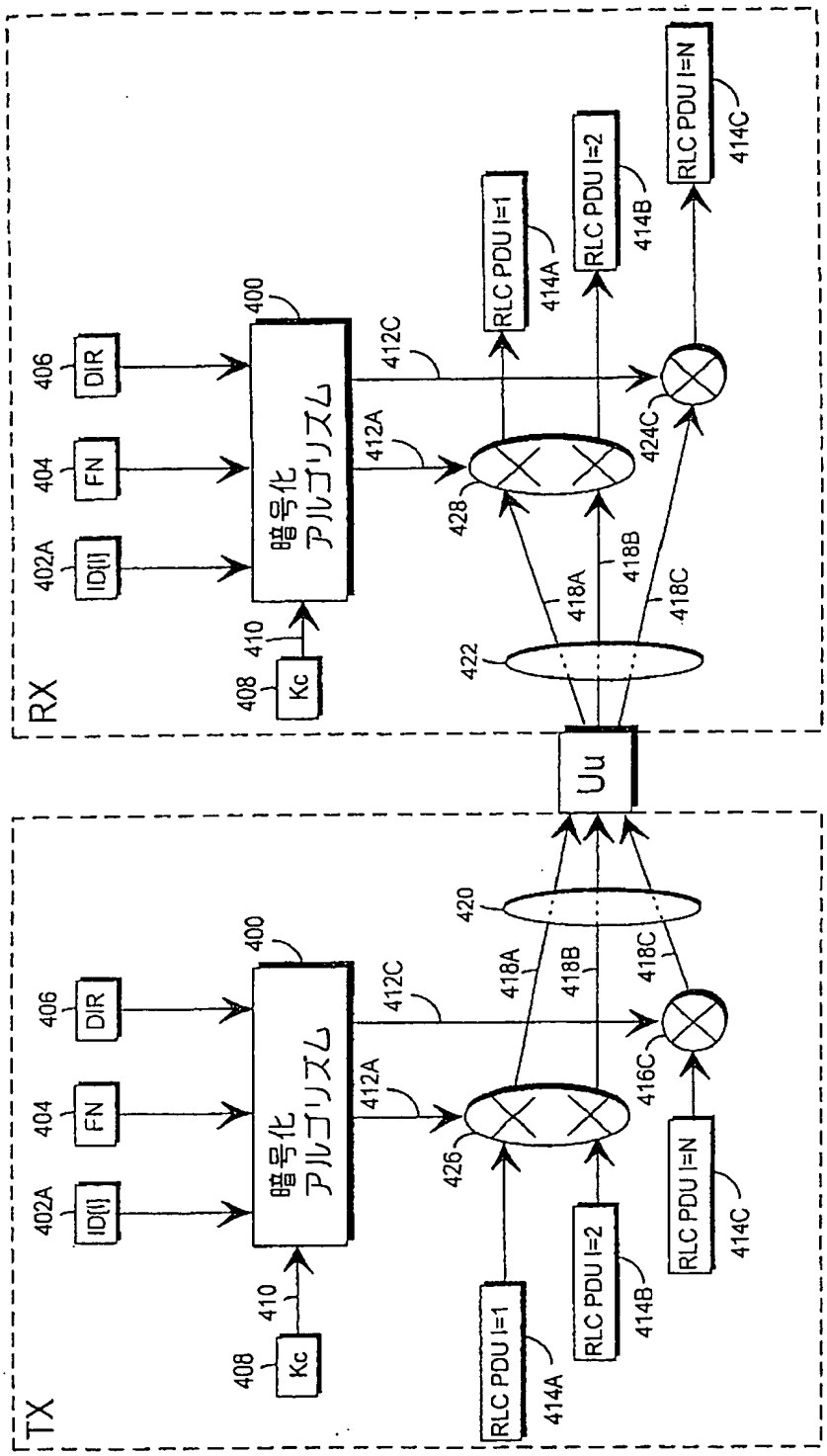

TX
RX
Uu
暗号化アルゴリズム
DIR
FN
ID[i]
Kc
RLC PDU I=1
RLC PDU I=2
RLC PDU I=N
400
402A
404
406
408
410
412A
412C
414A
414B
414C
416C
418A
418B
418C
420
422
424C
426
428

Fig 4B

【図４Ｃ】

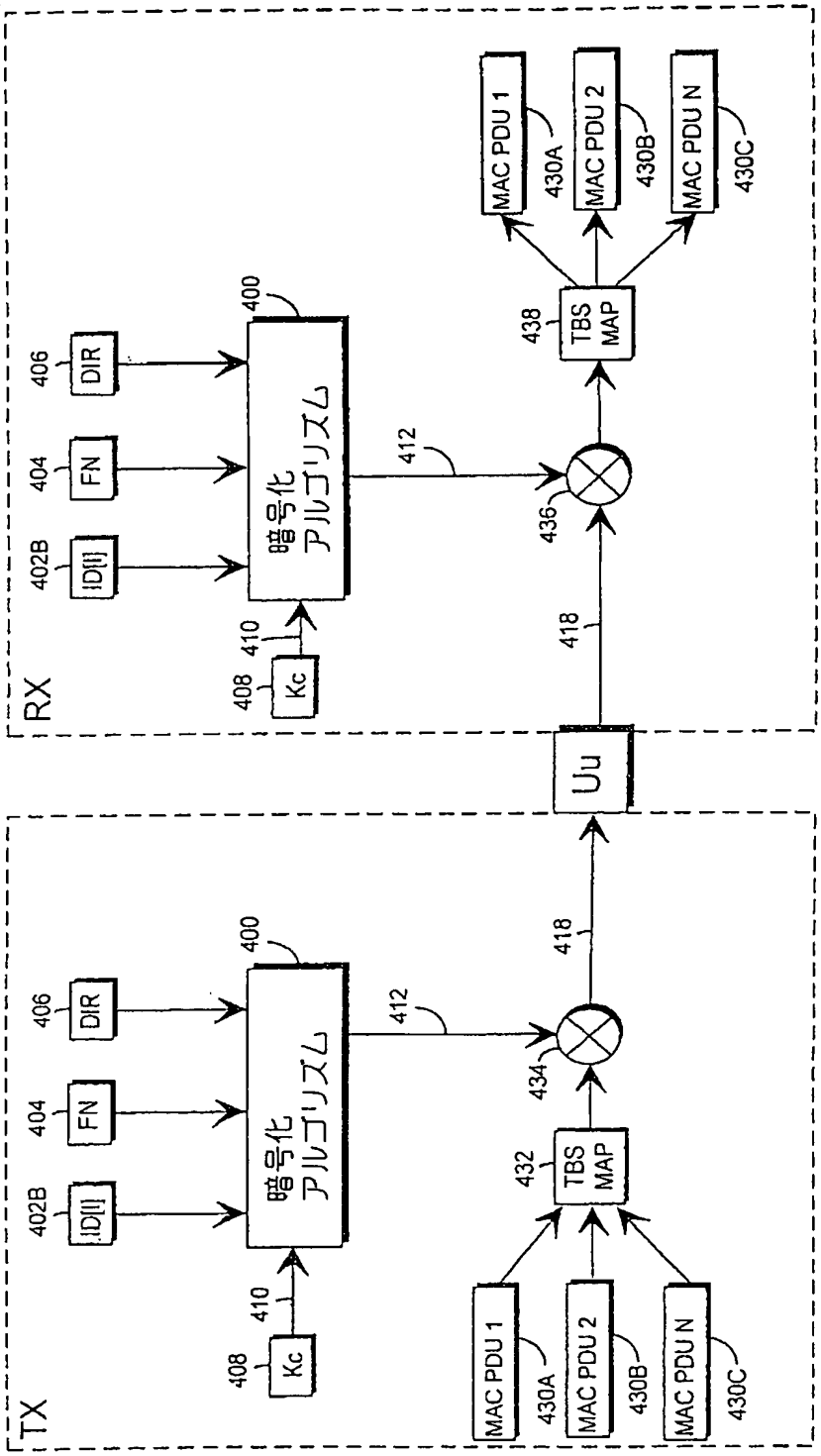

TX
RX
Uu
暗号化アルゴリズム
DIR
FN
IDII
Kc
TBS MAP
MAC PDU 1
MAC PDU 2
MAC PDU N
400
402B
404
406
408
410
412
418
430A
430B
430C
432
434
436
438

Fig 4C

【図５】

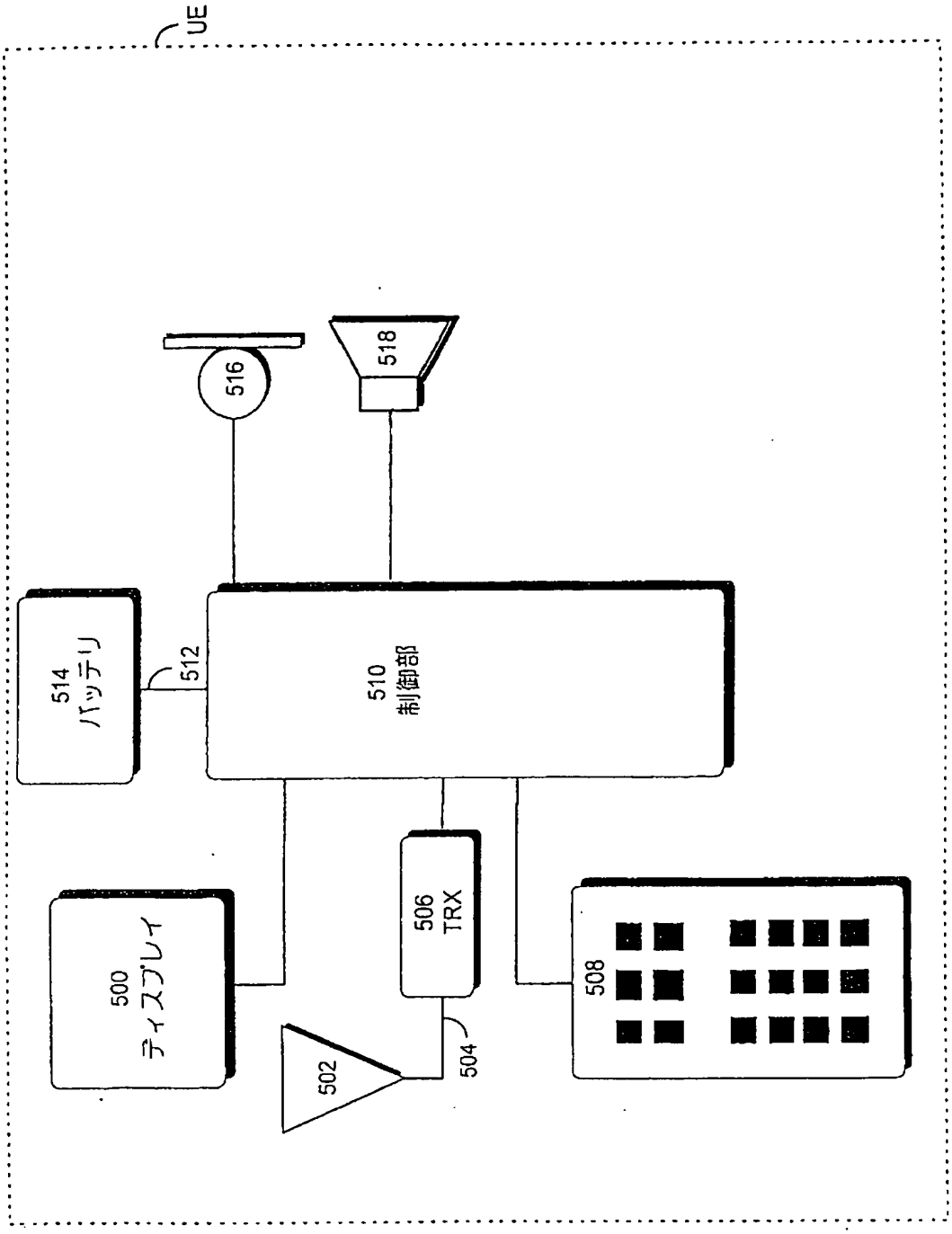


Fig 5

【図６】

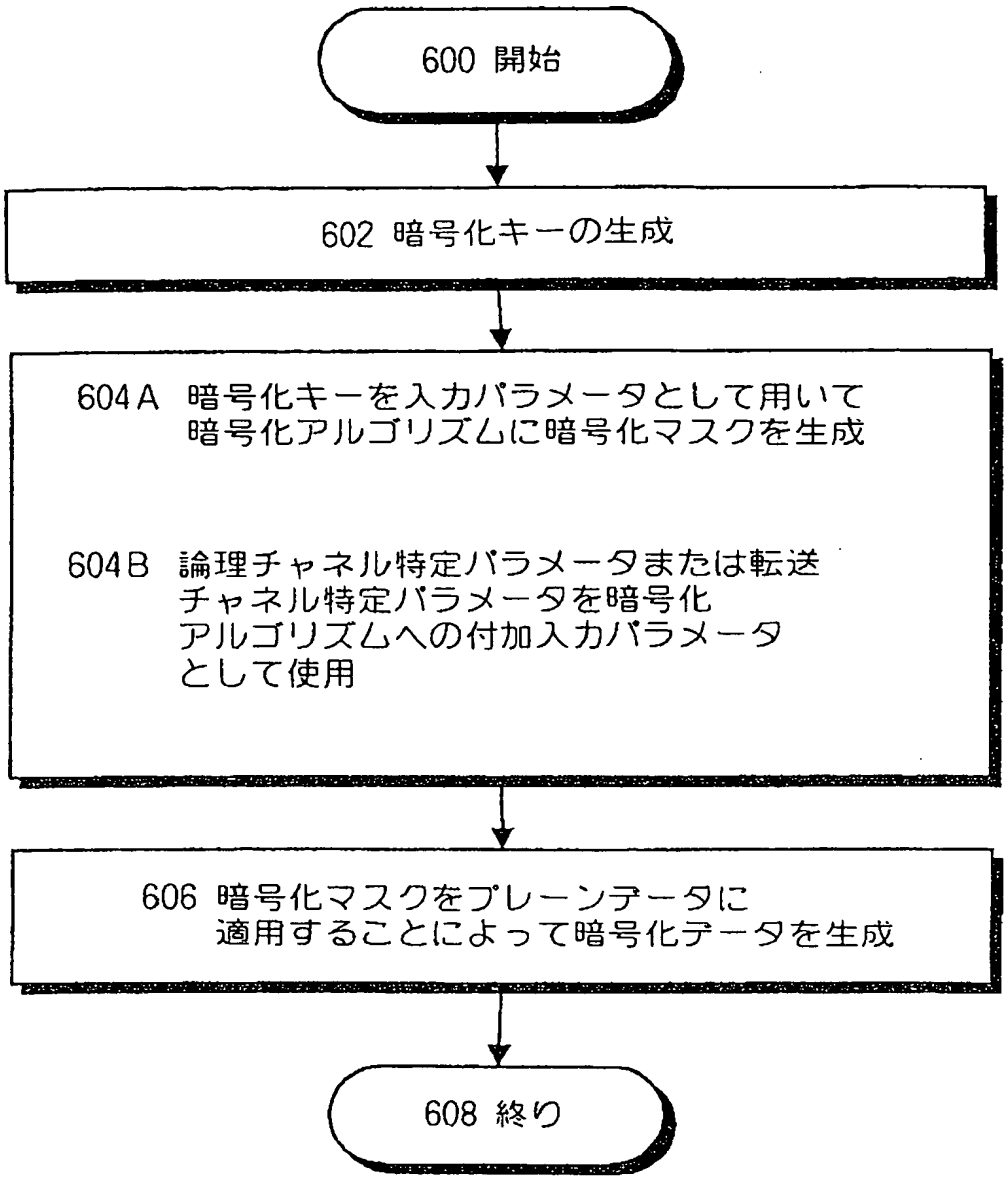

600 開始
602 暗号化キーの生成
604A 暗号化キーを入力パラメータとして用いて
暗号化アルゴリズムに暗号化マスクを生成
604B 論理チャネル特定パラメータまたは転送
チャネル特定パラメータを暗号化
アルゴリズムへの付加入力パラメータ
として使用
606 暗号化マスクをプレーンデータに
適用することによって暗号化データを生成
608 終り

Fig 6

【図７Ａ】

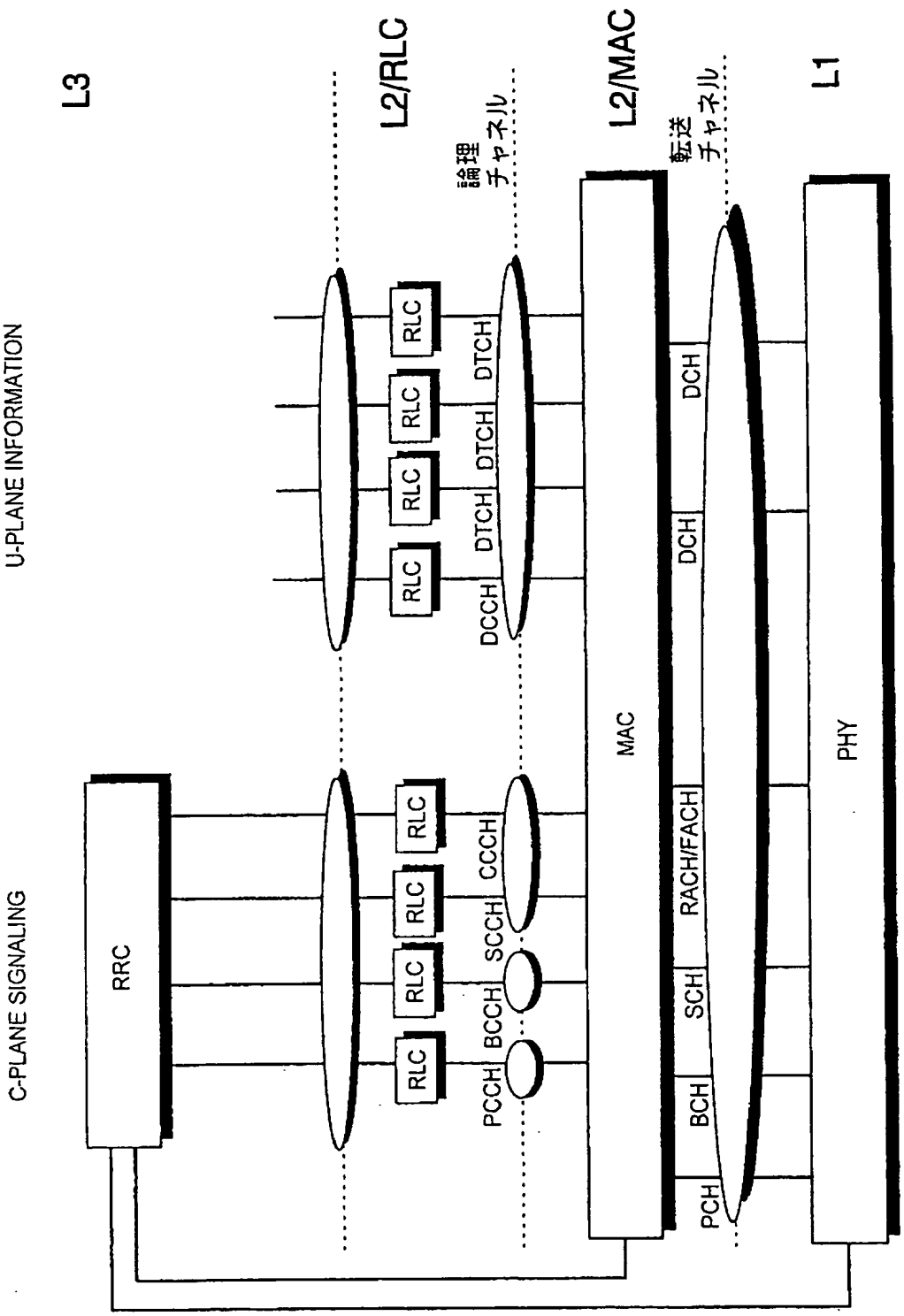

L3
L2/RLC
論理チャネル
L2/MAC
転送チャネル
L1
U-PLANE INFORMATION
C-PLANE SIGNALING
RRC
RLC
RLC
RLC
RLC
RLC
RLC
RLC
RLC
DCCH
DTCH
DTCH
DTCH
CCCH
SCCH
BCCH
PCCH
MAC
DCH
DCH
RACH/FACH
SCH
BCH
PCH
PHY

Fig 7A

【図７Ｂ】

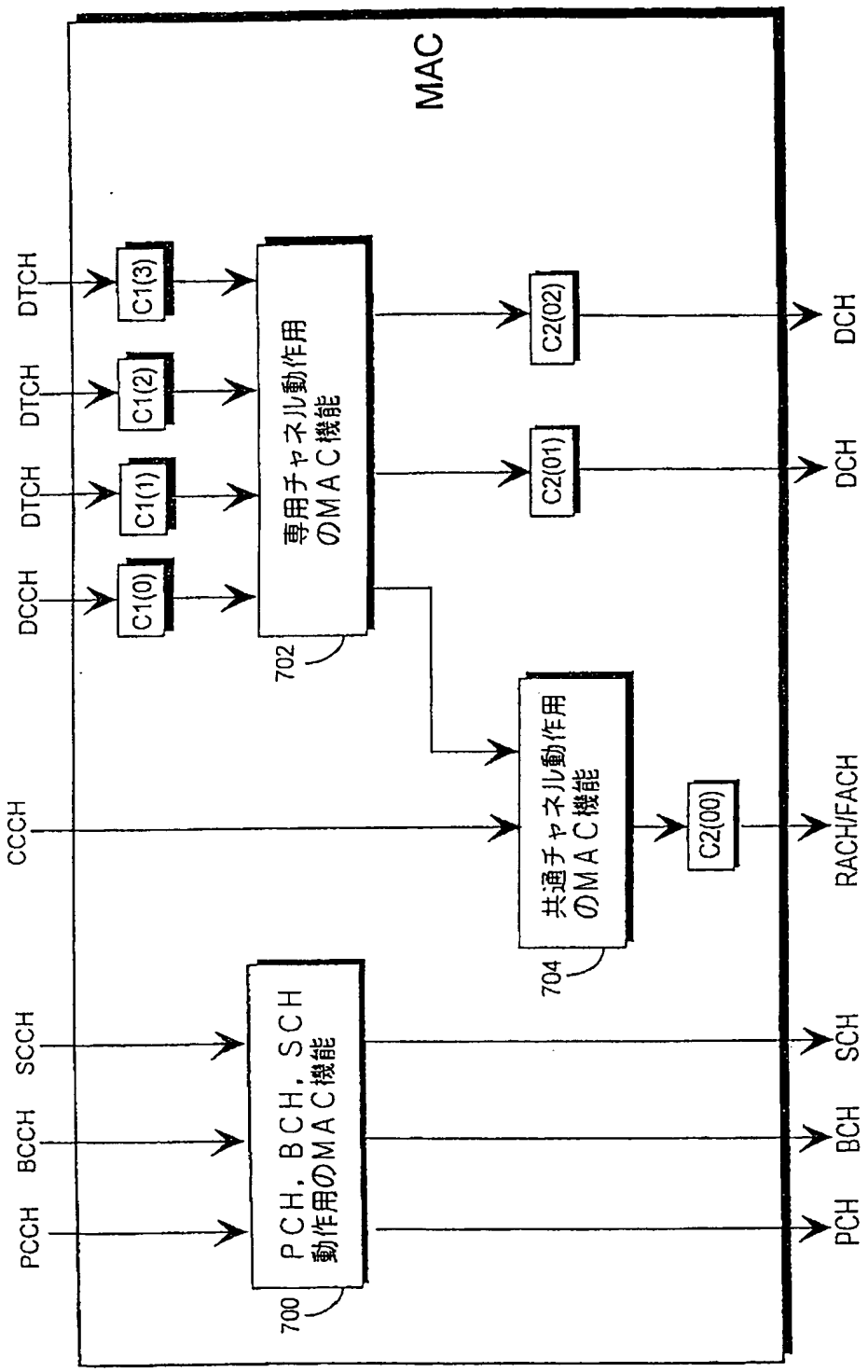

MAC
DTCH
DTCH
DTCH
DCCH
C1(3)
C1(2)
C1(1)
C1(0)
専用チャネル動作用のＭＡＣ機能
702
C2(02)
C2(01)
DCH
DCH
CCCH
共通チャネル動作用のＭＡＣ機能
704
C2(00)
RACH/FACH
SCCH
BCCH
PCCH
ＰＣＨ，ＢＣＨ，ＳＣＨ動作用のＭＡＣ機能
700
SCH
BCH
PCH

Fig 7B

【図７Ｃ】

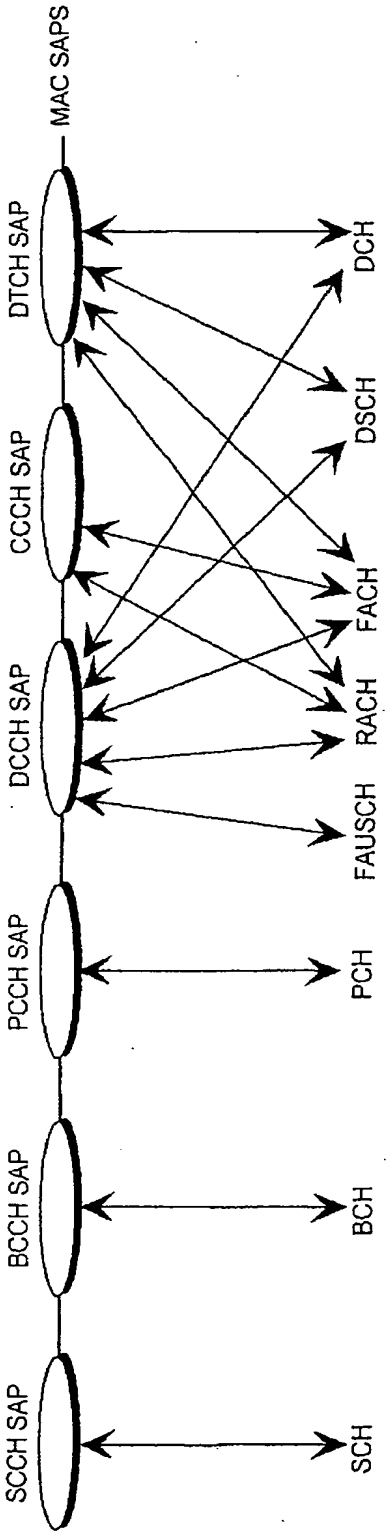

MAC SAPS
DTCH SAP
CCCH SAP
DCCH SAP
PCCH SAP
BCCH SAP
SCCH SAP
DCH
DSCH
FACH
RACH
FAUSCH
PCH
BCH
SCH

Fig 7C

【図８】

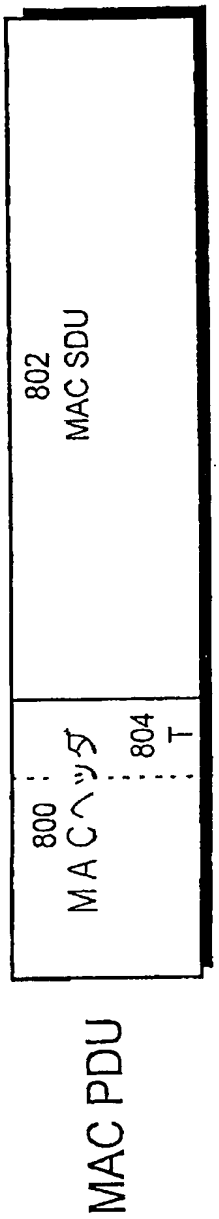


Fig 8

【国際調査報告】

1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00177

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/16
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9712461 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 3 April 1997 (03.04.97), claim 1	1,16,31
A		2-15,17-30, 32-45
	--	
A	US 5600722 A (T. YAMAGUCHI ET AL.), 4 February 1997 (04.02.97), see the whole document	1-45
	--	

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 August 2000	04 -08- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/AE Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT
Information on patent family members

02/12/99

International application No.
PCT/FI 00/00177

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9712461 A1	03/04/97	AU 7102196 A	17/04/97
		CA 2233463 A	03/04/97
		CN 1198278 A	04/11/98
		EP 0872078 A	21/10/98
		JP 11511629 T	05/10/99
		NZ 318911 A	29/06/99
		SE 506619 C	19/01/98
		SE 9503343 A	28/03/97
US 5600722 A	04/02/97	JP 7107083 A	21/04/95
		US 5604807 A	18/02/97

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW

Fターム(参考) 5J104 AA32 BA04 NA02
5K067 AA30 BB04 BB21 DD17 EE02 EE10 FF02 HH22 HH24 HH36 KK15